REDES BASADAS EN SOFTWARE COMO ESQUEMA DE CONECTIVIDAD Y ADMINISTRACION WAN EN ENTORNOS CORPORATIVOS

CESAR EDUARDO LUQUE QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
BOGOTÁ, COLOMBIA
MARZO DE 2021

REDES BASADAS EN SOFTWARE COMO ESQUEMA DE CONECTIVIDAD Y ADMINISTRACION WAN EN ENTORNOS CORPORATIVOS

CESAR EDUARDO LUQUE QUINTERO

Trabajo de grado presentado como requisito para optar al título de:
Especialista en redes de nueva generación

Director:
Mag. Iván Camilo Nieto Sánchez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
BOGOTÁ, COLOMBIA
MARZO DE 2021

DECLARACIÓN DE DERECHOS DE PROPIEDAD INTELECTUAL

Los autores de la presente propuesta manifestamos que conocemos el contenido del Acuerdo 06 de 2008, Estatuto de Propiedad Intelectual de la UNAD, Artículo 39 referente a la cesión voluntaria y libre de los derechos de propiedad intelectual de los productos generados a partir de la presente propuesta. Asimismo, conocemos el contenido del Artículo 40 del mismo Acuerdo, relacionado con la autorización de uso del trabajo para fines de consulta y mención en los catálogos bibliográficos de la UNAD.

Hay una fuerza motriz más poderosa
que el vapor, la electricidad y la energía
atómica: la voluntad.

Albert Einstein.

Agradecimientos

A mis padres, por infundir en mí los valores necesarios para enfrentar las adversidades y perseverar por los sueños, a mi familia por el respaldo constante; de la misma manera a todo el grupo docente de la universidad y profesionales del entorno laboral que apoyaron mi interés por la adquisición de nuevos conocimientos y nuevas habilidades que me permiten continuar en el crecimiento personal y profesional.

Resumen

El crecimiento exponencial de los productos ofertados por los proveedores de servicio a compañías y usuarios finales ha llevado al desarrollo de nuevas tecnologías, que permiten optimizar el uso de la infraestructura tecnológica y garantizar mayor grado de calidad en cada una de las aplicaciones que se transportan en la red. De esta forma, con el incremento en el uso de arquitecturas de software e infraestructuras como servicio (SaaS/IasS) por parte de las empresas se ha observado que las redes tradicionales no aseguran los factores de granularidad requerida para cumplir con los niveles de Qos esperado por los usuarios (Staff, 2016). En la búsqueda de una solución a estos inconvenientes surgen los diseños basados en software los cuales a través de su nuevo enfoque logra una reducción de costos y la optimización de recursos mediante la separación de los planos de control y de datos.

Teniendo en cuenta lo anteriormente expuesto, esta monografía se construye con el ánimo de identificar qué ventajas tienen las redes basadas en software con relación a los esquemas de red tradicionales. Las mejoras relacionadas se enfocan en nuevas características de conectividad y su esquema de administración bajo una plataforma centralizada.

Palabras claves: SD WAN, SDN, CISCO, FABRIC, UNDERLAY, OVERLAY, MPLS, OMP, IPSEC.

Abstract

The exponential growth of offered products by companies and end users have let the new technologies development, which allow optimizing the use of the technological infrastructure and guaranteeing a higher degree quality in transported applications in the network. On this way, the increasing in the use of "SaaS" architectures by companies, it has been observed traditional networks do not ensure the granularity required factors to meet the "Qos" expected levels by users (Staff, 2016). In the searching for a solution to these drawbacks, arise designs bases in softwares which through their new approach, achieves cost reduction and resource optimization through the control separation of and data planes.

Having in mind the previously exposed, this monograph is constructed with the aim of identifying advantages of software-based in compared networks to traditional network schemes. The related enhancements focus on new connectivity features and its management scheme under a platform centralized.

Keywords: SD WAN, SDN, CISCO, FABRIC, UNDERLAY, OVERLAY, MPLS, OMP, IPSEC.

Contenido

Introducción *1*

1.1. Definición del problema **2**

1.2. Justificación **2**

1.3. Objetivos **3**

1.3.1. Objetivo general 3

1.3.2. Objetivos específicos 3

Capítulo 2. Marco Conceptual y Teórico *5*

2.1. Limitaciones de las redes actuales 5

2.2. Complejidad 5

2.3. Políticas inconsistentes 6

2.4. Imposibilidad para escalar 6

2.5 Dependencia de los proveedores 6

2.6 Orígenes y evolución de las redes basadas en software SD WAN 7

2.7 Beneficios de las redes basadas en software SD WAN 8

2.7.1 Agilidad para el negocio 8

2.7.2 Ahorro del ancho de banda 9

2.7.3 Arquitectura optimizada para cloud 9

2.8 Transición hacia las redes basadas en SD WAN. 9

2.9 Regulación de servicios de comunicaciones en Colombia 10

Capítulo 3. Conceptos de arquitectura SD WAN *12*

3.1. Modelo y arquitectura de SD WAN 12

3.2. Data Plane (Plano de datos) 13

3.2.1. Bidireccional Forwarding Detection (BFD) 14

3.2.2. Overlay management protocol (OMP) 15

3.2.3 Ip Sec 16

3.2.4 Tecnologias de transporte en SD WAN 17

3.3 Control Plane (Plano de control) 18

3.3.1 Controladoras Vsmart 19

3.4 Management plane (Plano de administración) 20

3.5 Plano de orquestacion (Orchestration plane). 21

3.5.1 Equipo vbond 22

3.5.2 ZTP vs aprovisionamiento manual 23

4.1. Caracteristicas de seguridad en las redes basadas en software 25

4.2 Seguridad en el plano de control 26

4.2.1 Autenticación en el plano de contról 27

4.2.2 Encriptación en el plano de control 28

4.2.3 Integridad en el plano de contról 29

4.3 Seguridad en el plano de datos 30

4.3.1 Autenticación en el plano de datos 31

4.3.2 Encripcion en el plano de datos. 31

4.3.3 Integridad en el plano de datos....32

Capítulo 5. Separación de planos en SD WAN 33

5.1. Separación de los planos de control y de datos....33

5.2. Ventajas de la separacion de planos....33

6.1 El vmanage y sus caracteristicas....37

6.2 Funcionalidades generales del vmanage....38

6.2.1 Módulo de dashboard....39

6.2.2 Módulo de monitoreo....39

6.2.3 Módulo de configuración....40

6.2.4 Módulo de herramientas....41

6.2.5 Módulo de administracion....41

6.2.6 Módulo de análisis....42

6.3 Redes de transporte y plataforma de administración....43

6.4 Monitoreo de estadísticas y toma de decisiones....44

6.5 Redundancia a nivel de transporte....46

6.5.1 Redundancia mediante mallado (MESH)....46

6.5.2 Redundancia mediante tloc extensions....47

Capítulo 7. Implementación de una red SD WAN en un ambiente de producción. 48

7.1 Planteamiento del escenario....48

7.2 Consideraciones de diseño....48

7.2.1 Diseño del direccionamiento....49

7.2.3 Controladores y equipo vbond....50

7.3.1 Creación de los template....56

7.4 Pruebas de operatividad....58

Conclusiones....60

Bibliografía....62

Lista de figuras

Figura 1.Arquitectura SD WAN (Delivery & Era, 2019)
Figura 2. Data plane (Cisco, 2008)
Figura 3. Operación de OMP (Marshall, 2019)
Figura 4. IP Sec en SD WAN (Sanchis, 2018)
Figura 5. Ejemplo de red underlay (Arizmendi, 2014).
Figura 6. Color MPLS y LTE en SD WAN (Khabarov, 2019).
Figura 7.Actualizaciones desde el plano de control (Barozet, 2017).
Figura 8. Funcionamiento del vBond (Cisco, 2020a)
Figura 9. Funcionamiento de ZTP (Bialy, 2020)
Figura 10. Delitos informáticos en Colombia (Ceballos et al., 2019)
Figura 11. Autenticación en el plano de control (Cisco, 2019)
Figura 12. Hanshake DTLS (Ueno, 2020).
Figura 13. Algoritmo de una sola vía (Álvarez, 2016).
Figura 14. Seguridad en el plano de datos (Cisco, 2020a)
Figura 15. Sesiones de control con separación de planos (Barozet, 2017)
Figura 16. Topologías lógicas mediante políticas centralizadas (Barozet, 2017)
Figura 17. Pantalla Inicial Dashboard (Autor)
Figura 18. Módulo dashboard (Autor)
Figura 19. Módulo Monitor (Autor)
Figura 20. Módulo de configuración (Autor)
Figura 21. Modulo Tools (Autor)
Figura 22.Módulo de administración (Autor)
Figura 23. Módulo de Análisis (Autor)
Figura 24. Segmentación de vpn´s (Dclessons, 2020)
Figura 25. Esquema de colores en SD WAN (Autor)
Figura 26. Generación de estadísticas de transporte (Autor)
Figura 27. Transport mesh (Barozet, 2017)
Figura 28. Redundancia mediante TLOCS extensions (Barozet, 2017)
Figura 29. Conectividad entre sede y DC
Figura 30. Agregar controlador en plataforma
Figura 31. Opciones del controlador
Figura 32. Asignación de template a controlador
Figura 33. Proceso de asociación de template
Figura 34. Asignación de template a Vedge
Figura 35. Modificando configuración de template
Figura 36. Template para una sede
Figura 37. Template para data center
Figura 38. Sesiones de control
Figura 39. Trafico dentro del tunel
Figura 40. Establecimiento de sesiones BFD

GLOSARIO

Ip Sec: Protocolo encargado del aseguramiento de las comunicaciones sobre el protocolo e internet utilizando técnicas de cifrado y autenticación.

OMP (Overlay management protocol): Protocolo de enrutamiento para redes overlay que hace uso de túneles TLS/DTLS para compartir información entre los equipos de la red overlay.

TLS: Protocolo de seguridad de la capa de transporte diseñado para proporcionar seguridad a las conexiones TCP.

DTLS: Protocolo de seguridad de la capa de transporte encargado de proporcionar seguridad a las conexiones establecidas bajo UDP.

Vedge: Equipo del plano de datos encargado del reenvío de tráfico hacia los diferentes nodos involucrados en el intercambio de información.

Fabric: Termino usado para hacer referencia a toda la infraestructura de red sd wan.

MPLS: Protocolo de conmutación de etiquetas comúnmente utilizado como medio de transporte en redes de nueva generación. Segmenta el tráfico de los diferentes clientes en vrf´s.

VRRP: Protocolo de redundancia de primer salto empleado para la salida de tráfico. Este protocolo hace uso de los roles de master y backup para definir el equipo que tiene la prioridad.

On -premise: Infraestructura en la cual el cliente es responsable por todos los aspectos relacionados con la ejecución del software.

Hosted: Con este método de despliegue es el software sigue siendo propietarios del usuario final. Sin embargo, hace uso de proveedores de infraestructura para ejecutarlo.

Cloud: Los servicios cloud se encuentran manejados 100% por el proveedor de servicio. Es decir, el usuario final no es propietario del software ni de hardware.

TCLOC: Un tloc es la unión de un system ip, un color y una encapsulación para definir a donde debe ser enviado el tráfico en las redes SD WAN.

Vsmart: Equipos del plano de control que se encargan de dar la inteligencia de la red y de tomar las decisiones de enrutamiento.

GRE: Protocolo genérico de encapsulación capaz de transportar diferentes protocolos a través de otras redes. Este protocolo no encripta el tráfico por lo que es recomendable usarlo en conjunto con ip sec.

Control policy: Políticas configuradas en SD WAN para manipular el comportamiento de las conexiones del plano de control.

Data policy: Políticas configuradas en SD WAN para manipular el tráfico de datos enviado entre los equipos encargados del envío de paquetes.

Timer: Temporizador encargado de controlar los tiempos en los cuales se debe ejecutar alguna acción en la red.

Encriptación: Procedimiento realizado para convertir un texto en ininteligible y asegurar que no puede ser interpretado por un receptor no autorizado.

Hash: Transforma una entrada de datos en una nueva serie mediante el uso de un algoritmo matemático. El hash es un algoritmo de una sola vía, es decir, no se puede regresar al bloque inicial desde el resultado generado por el hash.

Netconf: Protocolo de configuración y administración de red estandarizado por la IETF. Hace uso de mensajes RPC como modelo de comunicación.

Diameter: protocolo diseñado para proporcionar servicios AAA en redes de nueva generación.

SSH: Protocolo de comunicación segura utilizado para gestionar equipos mediante una arquitectura cliente – servidor.

LTE: Tecnología inalámbrica de alta velocidad diseñada para permitir el acceso de los dispositivos móviles a internet.

GUI: Interfaz gráfica de usuario diseñada para facilitar la administración de dispositivos mediante el uso opciones interactivas.

ZTP. Zero touch provisioning es un mecanismo de autenticación y registro para nuevos equipos adicionados a la red SD WAN. La característica principal es su capacidad de realizar estas funciones de forma automática.

SD WAN: Tecnología de red overlay basada en software propietaria del fabricante Cisco.

Red overlay: Red de comunicaciones construida sobre otra red que permite el transporte y la interconexión entre nodos.

Red underlay: Red de transporte encargada de proporcionar conectividad de extremo a extremo entre nodos. Una red underlay puede estar compuesta por diferentes tecnologías convergentes.

Introducción

La constante evolución de los servicios en red ha llevado a las organizaciones a efectuar la migración de sus aplicaciones hacia arquitecturas cloud o hibridas para proporcionar un mayor dinamismo relacionado con factores como el crecimiento y la administración de la red. Este comportamiento ha llegado a mostrar algunas deficiencias de las redes tradicionales con relación a las nuevas y variadas aplicaciones utilizadas en los entornos corporativos.

Las deficiencias se observan especialmente en la poca flexibilidad que se obtiene en el momento en el que las condiciones de red cambian, cuando esto sucede es necesario modificar el comportamiento de la red mediante el análisis de las rutas alternativas y la selección de la mejor opción basado en las políticas previamente establecidas por el administrador de la red.

Consientes de estas limitaciones surgen las primeras ideas de crear un enfoque que proporcione una red con capacidad de medir los niveles de calidad y tomar decisiones sobre la mejor forma de enviar los datos desde el origen hasta el destino. Este nuevo paradigma es denominado, “redes basadas en software” donde se brinda mayor inteligencia a la red; además de la separación en los planos de datos y control. Con ello se adquiere un alto grado de escalabilidad y redundancia para mantener la disponibilidad de la red.

Las redes basadas en software se perfilan como la mejor alternativa de conectividad en los próximos años, así como la tecnología de mayor crecimiento en ambientes empresariales. Por lo tanto, este tipo de tecnología se adapta perfectamente a la arquitectura de redes de nueva generación ya que hace uso de la separación en planos facilitando la integración de forma transparente con las diferentes tecnologías de trasporte sin estar atada específicamente a ninguna de ellas.

Si bien en el mercado existen diferentes fabricantes que ofrecen soluciones de redes basadas en software en este documento se darán a conocer las características proporcionadas por el proveedor Cisco con su solución SD WAN.

Capítulo 1. Planteamiento del problema

En este primer capítulo se abordará el problema planteado, así como los objetivos que se pretenden cumplir con el desarrollo del presente documento. Así mismo, dentro del desarrollo de este capítulo se realizará una revisión conceptual para proporcionar una base teórica del estudio realizado.

1.1. Definición del problema

El incremento de nuevas aplicaciones y componentes en los entornos empresariales ha hecho que las compañías busquen obtener el mayor beneficio de sus esquemas de comunicaciones. Las empresas han iniciado un uso cada vez más amplio de las tecnologías en la nube y de aplicaciones en tiempo real que requieren de la máxima capacidad de las arquitecturas de conexión. Estas tecnologías experimentaron un crecimiento del 63% entre el 2012 al 2016 (CEPAL, 2014) y se espera que este comportamiento se mantenga mediante la inserción de nuevos servicios que materializan la transformación digital mediante la incorporación de modernos métodos para dar solución a necesidades económicas y sociales apalancados en el uso de las TIC (MinTIC, 2018). Con la evolución de la información que circula en la red y el valor que esta representa para las compañías, los esquemas de red tradicionales se han quedado rezagados debido a que las redes tradicionales no son capaces de satisfacer las demandas de las empresas que solicitan tecnologías que les permita superar los retos empresariales, reducir los gastos de mantenimiento y acelera sus procesos de digitalización(Reseller, 2018).

Por otra parte, en los esquemas tradicionales los esquemas de seguridad son administrados mediante el uso de diferentes modelos por ejemplo el X.800 que utiliza parámetros de seguridad generales y aumenta la complejidad en la red (Baluja, 2011). Estos estándares pueden dificultar las funciones de mantenimiento o actividades programadas sobre algún componente debido a que el amplio número de módulos y dimensiones con las que propone trabajar añade demora y complejidad a cualquier tarea de seguridad(Baluja, 2011).

1.2. Justificación

La dinámica evolutiva de los sistemas de comunicaciones ha creado la necesidad de desarrollar nuevas formas de conexión que proporcionen más y mejores beneficios tanto a empresas como a usuarios finales. En la actualidad, las tecnologías de comunicación a través de redes basadas en software (SDN) implementan algunas mejoras en aspectos en los cuales las redes tradicionales

presentaban deficiencias. La evolución natural de la red crea la necesidad de construir nuevos conocimientos en base a fuentes documentales especializadas que permiten la apropiación de conocimientos necesarios para implementar estos esquemas.

En los entornos corporativos cada vez es más necesaria la optimización de recursos y las redes de comunicaciones no son ajenas a esa problemática. En las empresas se ha empezado a identificar las dificultades que las implementaciones tradicionales presentan para efectuar funciones de administración y análisis de tráfico en los ambientes de producción que involucran aplicaciones que requieren un tratamiento especial. Estos inconvenientes han hecho que se vea a las redes basadas en software como una gran oportunidad hacia un avance en los modelos de comunicación.

Las redes basadas en software constituyen un gran universo dentro de las tecnologías de interconexión; existe la necesidad de conocer a profundidad las características y ventajas que proporciona este tipo de esquema. La presente monografía sirve como una fuente investigativa que permite identificar los fundamentos de este enfoque y evaluar el impacto de su implementación en cada una de las empresas donde se desee hacer uso de ella. Asimismo, la creación de estas fuentes documentales sirve de base para la elaboración de investigaciones relacionadas con la inteligencia de la red mediante políticas centralizadas o programación a través de APIS y lenguajes de alto nivel, las cuales son características soportadas en esta arquitectura pero que todavía no han sido exploradas en su totalidad.

1.3. Objetivos

1.3.1. Objetivo general

Comprender las ventajas de la implementación y administración de redes basadas en software en los entornos corporativos mediante la revisión de fuentes documentales que facilitan el entendimiento de los despliegues en esquemas de conectividad WAN.

.

1.3.2. Objetivos específicos

- Analizar la relación existente entre los componentes involucrados en esta

arquitectura, estableciendo el proceso de comunicación WAN en las redes basadas en software.

- Establecer el alcance de las características de seguridad en las redes basadas en software y el uso de sus protocolos como mecanismo de protección ante ataques a la red.
- Describir los beneficios que representa la separación de planos en la solución de problemas de escalabilidad que presentan las redes tradicionales.

- Detallar las funciones disponibles en la plataforma de administración orientadas a la gestión por parte de los operadores de red.

Capítulo 2. Marco Conceptual y Teórico

En este capítulo se exponen los referentes teóricos que sirven como referencia conceptual para comprender el problema planteado, así como la solución propuesta.

2.1. Limitaciones de las redes actuales

Las arquitecturas de red convencionales proporcionaban una gran eficiencia en el transporte de información para arquitecturas empresariales que basaban sus flujos de tráfico en la arquitectura cliente servidor. Esta arquitectura se fue viendo impactada gradualmente por el cambio en la naturaleza de las aplicaciones, ya que en la mayoría de los casos se inició un proceso de migración hacia ambientes Cloud con lo cual las redes tradicionales fueron mostrando sus falencias por su falta de flexibilidad y capacidad de adaptación a estos nuevos escenarios.

Dentro de las limitaciones de las redes actuales tenemos:

2.2. Complejidad

La tecnología de redes hasta la fecha ha consistido en gran medida en conjuntos discretos de protocolos diseñados para conectar host confiablemente sobre distancias arbitrarias, velocidades de enlaces y topologías. Para cumplir necesidades técnicas y de negocios la industria ha evolucionado los protocolos para ofrecer mayor rendimiento, confiabilidad y una seguridad más estricta. Los protocolos tienden a definirse de manera aislada y cada uno resuelve un problema específico, pero sin ninguna abstracción fundamental.

Esto ha resultado en una de las principales limitaciones de las redes de hoy en día, la complejidad. Por ejemplo, para mover o adicionar algún dispositivo el equipo de IT debe tocar múltiples switches, routers, firewalls, portales de autenticación web etc. y debe actualizar ACL´s, VLAN´s calidad de servicio (Qos) y otros mecanismos basados en protocolos. Adicionalmente la topología, los fabricantes, los modelos y las versiones de software deben ser tenidos en cuenta. Esto hace complejas las redes de hoy en día y relativamente estáticas para minimizar el riesgo de fallas(O.N.F., 2012) .

2.3. Políticas inconsistentes

Para implementar una política de red o realizar un cambio de política ante el cambio de un equipo es necesario aplicar cambios sobre diversos gestores o equipos enfocados a pequeños procesos que hacen parte del servicio completo. Es decir, no existe la posibilidad de políticas centralizadas que permitan una rápida gestión de los cambios y un despliegue automático en los equipos que realizan las acciones o toman decisiones con base en esa política.

Esta falencia también puede generar una alta complejidad a la hora de diseñar un plan de acción relacionado con la modificación de políticas, o en algunos casos generar incidentes asociados a comportamientos no esperados en actividades programadas.

2.4. Imposibilidad para escalar

La fuerte demanda de nuevos servicios ha hecho que la red también se extienda a niveles no imaginados. Este crecimiento de la red trae consigo la necesidad de instalar más equipos que deben ser configurados y gestionados adecuadamente para proporcionar los servicios. Este patrón de crecimiento hace que la red no proporcione los niveles de escalabilidad para el patrón de datos dinámico que se maneja hoy en día.

Entre el 80 y el 95% de las operaciones de red se siguen realizando de forma manual. Esto supone un gasto de 60.000 millones de dólares a escala global sólo en mantenimiento y operación. Tres veces más del presupuesto que las organizaciones destinan a actualizar tecnológicamente la propia red (Infante, n.d.).

2.5 Dependencia de los proveedores

Los Carrier y las empresas buscan desplegar nuevas capacidades y servicios en respuesta a las necesidades cambiantes del negocio o demandas del usuario. Sin embargo, su capacidad de respuesta se ve obstaculizada por los proveedores o ciclos de productos los cuales pueden ir hasta los tres años o más. Esta discordancia entre requerimientos del mercado y capacidades de la red ha traído a la industria hasta a un punto de inflexión. En respuesta la industria ha creado las redes definidas por software que tienen una arquitectura diseñada con estándares asociados (O.N.F., 2012).

2.6 Orígenes y evolución de las redes basadas en software SD WAN

La evolución de las redes basadas por software nace como una iniciativa por parte de los investigadores para dar mejores niveles de abstracción y la capacidad de programar las redes a través de APIS.

La historia de estas redes está dividida en tres etapas cada una con sus propias contribuciones (Feamster, 2014).

Redes Activas (desde mediados de la década de 1990 hasta comienzos de la década del 2000)

En esta etapa se introdujeron funciones programables en la red lo que condujo a una mayor innovación.

Separación del plano de control del plano de datos (de 2001 a 2007)

En esta etapa se realizó el desarrollo de interfaces abiertas entre el plano de control y el plano de datos

Creación de API flow (desde 2007 hasta 2010)

Se realizó la primera adopción generalizada de una interfaz abierta logrando de esta forma la que la separación del plano de control y datos fuera escalable.

Los orígenes de SD WAN se remontan al año 2007 cuando se llevó a cabo en la universidad de Stanford una reunión entre expertos en networking para analizar el presente y futuro de las redes. Este proyecto fue denominado “Clean slate” debido a la metodología de trabajo utilizada que consistían en definir como se podría construir una red desde ceros, pero con el conocimiento actual con que se contaba en ese momento.

En este grupo de trabajo se constata que parte del éxito del protocolo IP, que consiste en compartir entre todos los nodos el conocimiento y la toma de decisiones de encaminamiento, iba camino de convertirse en un cáncer para la red. La razón es que todos y cada uno de los miles de nodos que componen la red necesitan ser programados con una sintaxis compleja y propietaria, con el impacto en la gestión de red que ello supone (Gil, 2018).

A partir de ese año se puede considerar el nacimiento de las redes basadas en software ya que se trabajó de manera constante en la separación de los planos de control y de datos. Estos esfuerzos llevaron a que la ONF (Open Networking Foundation) tomara las funciones de desarrollo y estandarización de este tipo de redes a partir del año 2012.

Las perspectivas de las redes basadas en software SD WAN son prometedoras ya que según las encuestas realizadas por portales especializados demuestran que la tendencia por parte de las empresas es realizar la migración de sus servicios a la nube. Según (Vector, 2018) “En 2020 ese porcentaje subirá al 60% cuando se refiera a infraestructura de TI y representará entre el 60% y el 70% de todos los gastos de software, servicios y tecnología”. Este comportamiento hace que las tecnologías basadas en software se conviertan en una solución atractiva para las compañías que se encuentran inmersas en procesos de renovación tecnológica.

2.7 Beneficios de las redes basadas en software SD WAN

Sin duda cada día aumenta el despliegue de tecnologías basadas en software por parte de las empresas que requieren hacer un uso óptimo del ancho de banda a la vez que proporcionan al negocio una optimización de Opex (Operating Expense) y Capex (Capital Expenditures) mediante la reutilización de hardware y la reducción del tiempo dedicado a funciones de configuración y mantenimiento.

Esta optimización de recursos y capital humano han sido solo algunos de los puntos que llaman la atención de los CIO´s de las empresas, ya que además de esto tenemos los siguientes beneficios que fortalecen aún más el cambio de redes tradicionales a redes basadas por software para organizaciones distribuidas (Rodríguez, 2008).

2.7.1 Agilidad para el negocio

El rápido despliegue de servicios WAN a oficinas remotas, sin necesidad de enviar personal de TI a desplegarlos on-site. El ancho de anda se puede añadir o reducir fácilmente en función de las necesidades del negocio.

2.7.2 Ahorro del ancho de banda

La conexión a internet está disponible fácilmente, es rápida de desplegar y tiene un costo mucho menor que el equivalente en redes MPLS. SD WAN ofrece los beneficios de fiabilidad y seguridad de los servicios WAN al precio de internet.

2.7.3 Arquitectura optimizada para cloud

SD-WAN elimina los inconvenientes y penalidades tradicionales de la red MPLS y equipara la seguridad, rendimiento y conectividad entre la oficina y la nube, lo que mejora de forma considerable a experiencia de los usuarios en las oficinas remotas cuando están usando aplicaciones que utilizan el software como servicio (Saas) o que se basan en cloud.

2.8 Transición hacia las redes basadas en SD WAN.

Existen tres estrategias para realizar los despliegues de las redes SD WAN en los entornos corporativos. Cada una de estas estrategias puede ser aplicada a las organizaciones de acuerdo a las necesidades que mejor se adapten a las estrategias de operación TI.

- Do it Yourself (DIY)

En esta estrategia de despliegue las organizaciones realizan directamente las funciones de implementación de los servicios SD WAN con su personal de TI. Este esquema es mayoritariamente utilizado por las empresas que cuentan con los suficientes recursos financieros y técnicos para hacerse cargo de la gestión y el mantenimiento de la red.

Uno de los escollos de una DIY SD WAN es tener que reducir al mínimo el número de proveedores de equipos utilizados para no tener que recurrir a tecnologías puente adicionales de dos proveedores diferentes. Esto también crear trabajo adicional potencialmente perturbador en el mantenimiento del sistema elegido, ya que solo el personal con los conocimientos técnicos será capaz de implementar cambios o abordar cuestiones tecnológicas (Lanner, n.d.).

- Totalmente Gestionado

El modelo gestionado entrega la responsabilidad de la implementación y administración de la red al proveedor de servicios. En este tipo de despliegue se definen acuerdos de nivel de servicio entre las partes involucradas para garantizar las características de calidad de servicio que debe garantizar el proveedor hacia el cliente final.

- Hibrido

Los modelos híbridos de despliegue se centran en la cogestión de la solución SD WAN elegida tanto por el cliente como por su proveedor de servicios de red.

En un modelo hibrido las empresas y los negocios son libres de crear sus propias políticas de seguridad y aplicaciones para el tipo de despliegue especifico que tengan en mente, mientras que su proveedor de servicios gestionados gestionara la experiencia del cliente y los aspectos de conectividad, al tiempo que garantizan cualquier SLA de red (Lanner, 2019.).

2.9 Regulación de servicios de comunicaciones en Colombia

En Colombia los servicios de comunicaciones están sujetos a vigilancia por parte de tres entidades las cuales reglamentan y regulan el mercado para evitarlas prácticas indebidas o que se vulneren los derechos de los consumidores de servicios.

En primer lugar, se encuentra la comisión de regulación de comunicaciones (CRC) que es el órgano encargado de promover la competencia, evitar el abuso de posición dominante y regular los mercados de las redes y los servicios de comunicaciones; con el fin que la prestación de los servicios sea económicamente eficiente, y refleje altos niveles de calidad(MinTIC, 2020). El marco jurídico se encuentra en la resolución 3011 de la CRC así como la aplicación del régimen de protección al consumidor.

En segunda medida se encuentra la Superintendencia de industria y comercio que se encarga de vigilar la observancia de las disposiciones contenidas en el estatuto del consumidor, Ley 1480 de 2011, en tal virtud tramita las denuncias que se presentan e inicia investigaciones de oficio tendientes a establecer su contravención. En este campo tiene facultades administrativas para ordenar la suspensión de conductas ilegales, sancionatorias para reprimir a los infractores y jurisdiccionales para resolver sobre la garantía mínima presunta.(SIC, n.d.)

Finalmente se encuentra el ministerio de las tecnologías de la información MinTic el cual se encarga de diseñar y promover las políticas sobre las cuales se deben regir los servicios de comunicaciones que sirve como la hoja de ruta para la implementación de nuevas tecnologías en el país.

Es de aclarar que los entes tienen funciones distintas e intervienen de manera autónoma de acuerdo con sus competencias.

Capítulo 3. Conceptos de arquitectura SD WAN

En este capítulo se hará un reconocimiento de los componentes que hacen parte de las soluciones de redes basadas por software SD WAN. A su vez se hace un reconocimiento de las características de separación de planos para proporcionar flexibilidad y facilitar la administración de las redes corporativas.

3.1. Modelo y arquitectura de SD WAN

Las redes definidas en software SD WAN están diseñadas para facilitar la creación de redes flexibles que puedan adaptarse a los constantes cambios en los patrones de tráfico generados por las diferentes aplicaciones dentro de la red. Para lograr los niveles de escalabilidad deseados, se creó un diseño basado en la separación de planos en donde cada plano tiene funciones específicas dentro de toda la operación de SD WAN. Los planos definidos en esta nueva arquitectura son el data plane, el control plane, el management plane y el Orchestration plane.

Esta separación en planos ha facilitado el uso de las redes basadas en software (SDN) en integracion con diferentes tecnologías de transporte como los son MPLS, Internet, 4G, y LTE entre otras, proporcionando así óptimos niveles de escalabilidad al mismo tiempo que mantiene la independencia con respecto a las capas subyacentes. El modelo de separación en planos también fortalece las características de seguridad mediante el uso de protocolos especializados en este aspecto en cada plano dentro de la arquitectura.

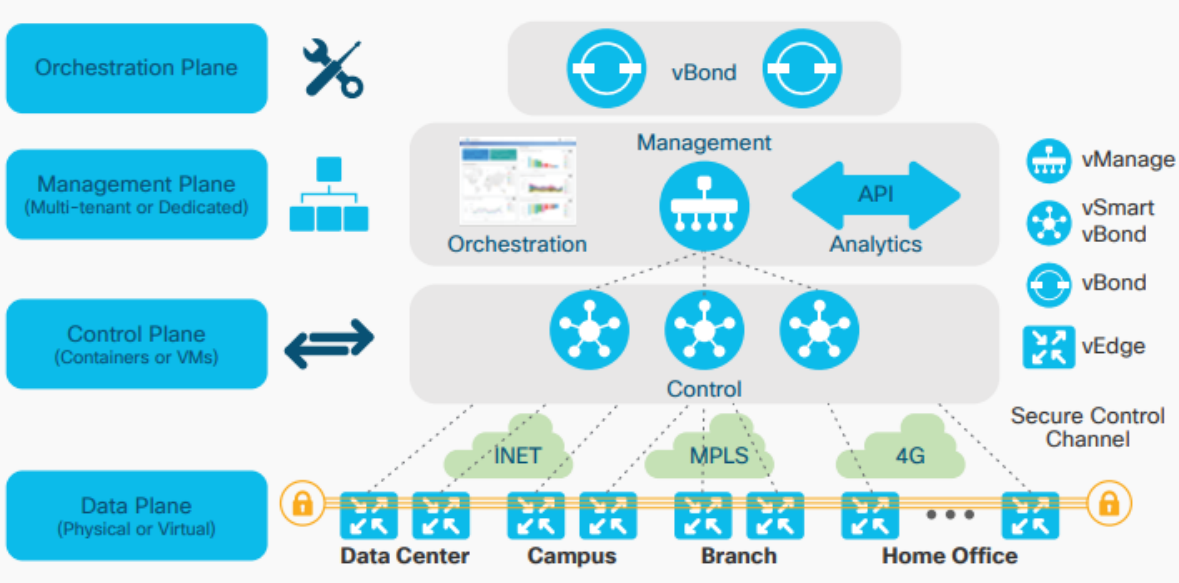


Figura 1.Arquitectura SD WAN (Delivery & Era, 2019)

Dentro de los componentes de SD WAN encontramos los equipos vedge, los vsmart, el vmanagement y los vbond. Cada uno de estos componentes están diseñados para realizar tareas específicas.

Las tecnologías de red basadas en software hacen parte de los modelos overlay, es decir, son redes virtuales que están configuradas sobre una red física y hace uso de protocolos de encapsulación para el establecimiento de túneles entre los nodos finales. La red underlay hace referencia a la red física proporcionada por los proveedores de servicio dentro de las cuales es común encontrar despliegues de de MPLS, 3G, LTE, Internet etc. En la terminología de SD WAN las redes físicas son conocidas como “colores” y son usadas por el overlay de acuerdo a las políticas creadas en el plano de control.

3.2. Data Plane (Plano de datos)

La función del plano de datos es realizar el envío de paquetes a través de la red para permitir la comunicación entre los diferentes nodos. En las redes tradicionales este envío es realizado en base a la tabla de enrutamiento que posee cada equipo o en base a la distribución de etiquetas en el caso de redes MPLS. A diferencia de las redes tradicionales en este nuevo modelo de red las decisiones de enrutamiento

son tomadas en un plano diferente y son comunicadas hacia el plano de datos a través del protocolo OMP.

En el caso de SD WAN, en el plano de control se encuentran los equipos V-Edge o C-Edge quienes se encargan del reenvío de datos de extremo a extremo optimizando los niveles de seguridad mediante el establecimiento de túneles IP SEC por donde es enviada la información. De esta forma se implementa la autenticación, la encriptación y la integridad sobre los datos transmitidos.

Figura 2. Data plane (Cisco, 2008)

En el plano de control se pueden encontrar los protocolos tradicionales como OSPF, BGP EIGRP, sin embargo, la distribución de información de enrutamiento dentro de los componentes de SD WAN se realiza mediante el uso del protocolo OMP.

3.2.1. Bidireccional Forwarding Detection (BFD)

Una de las grandes ventajas de las redes basadas en software SD WAN es su capacidad de reaccionar ante factores que generen una degradación de las condiciones inicialmente establecidas en la política centralizada.

Esta nueva tecnología establece sesiones BFD entre los equipos del plano de datos para censar las condiciones de jitter, latencia, MTU y pérdida de paquetes para tomar decisiones en base a los valores recopilados. Las sesiones BFD son establecidas dentro del túnel IPSEC y utilizan intervalos de saludo o sondeo para identificar el estado de canal.

Con esta funcionalidad se garantiza que los medios de transporte proporcionen los niveles de calidad requeridos. Dado el caso que los parámetros detectados por BFD estén por fuera del rango previamente establecido, la red está en capacidad de conmutar automáticamente el tráfico hacia otro canal que si garantice la calidad requerida por las aplicaciones. Esto le proporciona un grado de inteligencia a la red ya que puede efectuar cambios en su comportamiento sin la intervención del personal y de esta forma mejorar la administración y el performance de la red.

3.2.2. Overlay management protocol (OMP)

Para que la red SD WAN pueda proporcionar conectividad de extremo a extremo es necesario que de alguna forma comparta la información de enrutamiento hacia todos los equipos del plano de control. El protocolo encargado de realizar esta función es el Overlay managament Protocol (OMP).

Como se mencionó con anterioridad una de las ventajas de SD WAN es la separación de los planos de datos y de control, por lo que en esta arquitectura la inteligencia a nivel de enrutamiento se realiza en la capa de control y ésta a su vez anuncia la información de enrutamiento hacia los equipos del plano de datos.

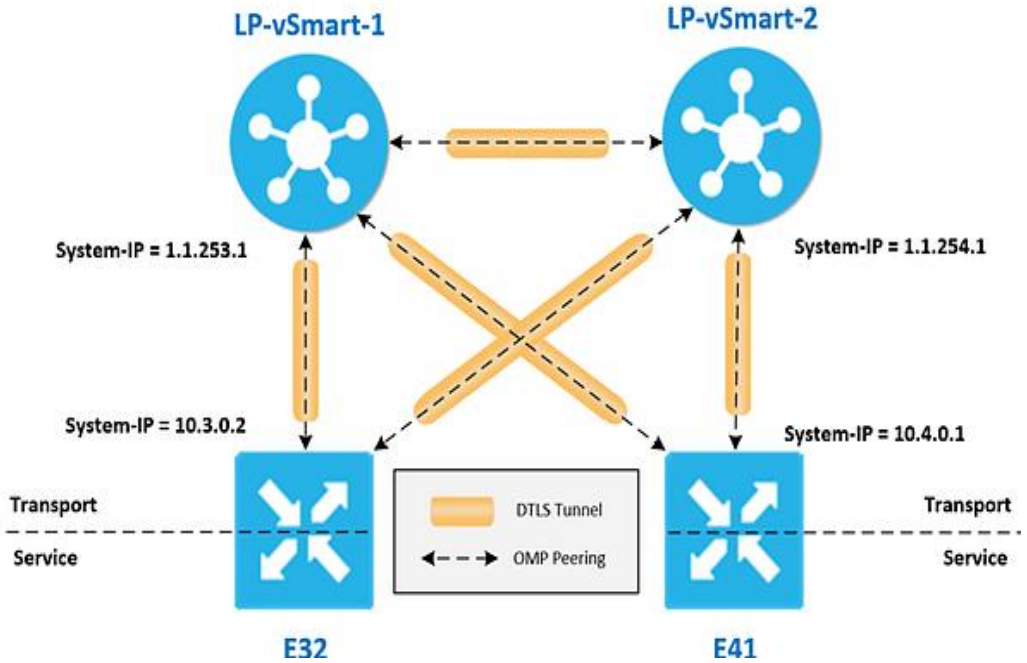


Figura 3. Operación de OMP (Marshall, 2019)

Para iniciar el intercambio de información de enrutamiento previamente se establecen túneles DTLS entre los equipos alojados en el plano de control y los equipos V-Edge o C-Edge encargados del plano de datos. Una vez establecido el túnel DTLS el protocolo OMP forma una relación de vecindad entre los equipos e inicia el proceso de anuncio de rutas.

OMP puede anunciar tres tipos de rutas; las rutas OMP que son los prefijos asociadas a las VPN de servicios. Los TLOC que son rutas asociadas a transporte físico y finalmente las rutas de servicio que corresponde a la información de los diferentes servicios cliente encontrados en SD WAN.

3.2.3 Ip Sec

Ip sec se empezó a utilizar en redes de gran tamaño a mediados de los años 2000, especialmente en las redes DMVPN para proporcionar seguridad y garantizar un mejor rendimiento de los servicios mediante el aseguramiento de condiciones como el jitter, latencia, perdida de paquetes y control de ráfagas(Cisco, 2019)

Dentro de la arquitectura SD WAN, IP Sec toma un rol fundamental en el plano de datos ya que se encarga de establecer túneles dinámicamente entre los diferentes puntos proporcionando un medio seguro y controlado para el envío de datos de cada una de las vpn configuradas dentro de la solución.

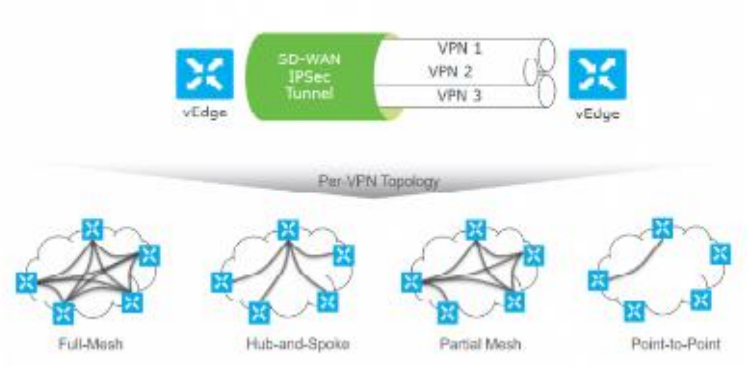


Figura 4. IP Sec en SD WAN (Sanchis, 2018)

Las diferentes topologías lógicas que se pueden configurar dentro de esta solución son diseñadas y anunciadas desde el plano de control hacia el plano de datos a

través del protocolo OMP y basadas en las políticas centralizadas en donde se definen las reglas para comunicación entre equipos. Esta característica le proporciona flexibilidad a la red en los escenarios en donde es necesaria la instalación de una nueva sede ya que los nuevos túneles Ip Sec se configurarán automáticamente en base a la política de control establecida.

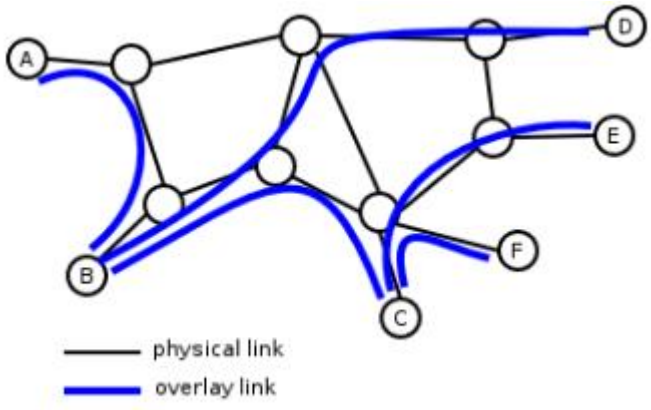


Figura 5. Ejemplo de red underlay (Arizmendi, 2014).

Otra función importante de Ip Sec dentro de la tecnología SD WAN es ocultar los saltos de la red underlay, es decir que el tráfico fluye entre el nodo origen y el nodo destino sin percatarse de la tecnología de transporte que se está usando. Esta característica contribuye a la flexibilidad y escalabilidad de este nuevo esquema de red.

3.2.4 Tecnologias de transporte en SD WAN.

Las tecnologías de transporte o mejor conocidas como redes underlay juegan un papel importante en la masificación de las redes basadas en software debido a que proporcionan la estructura física sobre la cual se despliegan los túneles de las nuevas redes underlay. De esta forma se aprovechan los avances tecnológicos que se han dado a lo largo de los años en este tipo de redes, así como el cubrimiento geográfico que han logrado a través de los años. Todo esto ha generado un impacto positivo en los usuarios de esta tecnología ya que de acuerdo a (IBM, 2018) aproximadamente el 30% de los participantes en una encuesta empresarial vieron que obtuvieron más de un 20% de ahorros generales.

Desde el punto de vista de SD WAN las redes de transporte se conocen como colores, por lo que cada tecnología de transporte WAN asignada a un equipo del

plano de datos se asocia a un color. Los colores disponibles son 3g, internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1, private2, private3, private4, private5, private6, public-internet, red y silver (Cisco, 2020b). Este modelo de colores facilita la configuración de la red overlay sobre diferentes tecnologías de transporte, pero conservando la gestión y administración centralizada.

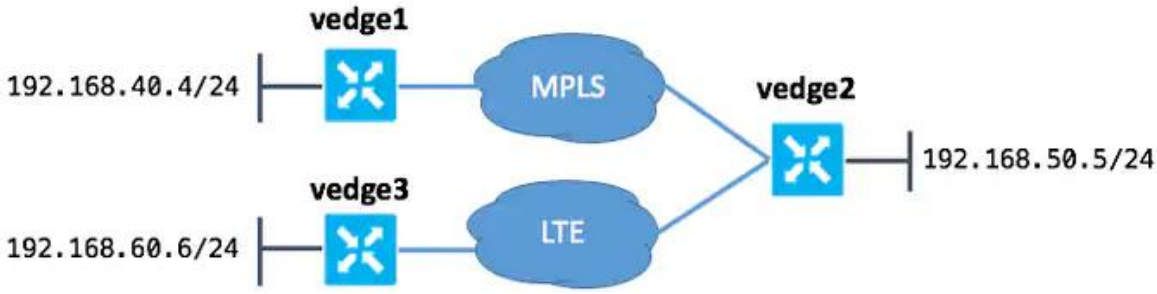


Figura 6. Color MPLS y LTE en SD WAN (Khabarov, 2019).

En la gráfica anterior se observa al equipo vedge2 utilizando un esquema de dos colores que forman el underlay. En este caso SD WAN puede establecer una red overlay mediante el uso de túneles IP Sec y posteriormente establecerá sesiones BFD entre los diferentes puntos de la red.

El trafico generado entre sedes puede ser balanceado entre los diferentes colores para optimizar al máximo las capacidades de cada uno de los transportes y garantizar mecanismos de redundancia en caso de falla alguno de los enlaces. La solución que más se emplea en los ambientes corporativos es el uso de MPLS e internet como medios de transporte, esta combinación proporciona los niveles de confiabilidad de las redes de conmutación de etiquetas y el bajo costo de las conexiones a internet.

3.3 Control Plane (Plano de control)

Una característica fundamental de las redes de nueva generación es la capacidad de separar las funciones en un plano independiente para facilitar la toma de decisiones y la interconexión con redes de diversas tecnologías por lo tanto SD WAN se amolda perfectamente a esta situación haciendo uso de su plano de control.

En las redes basadas en software y en especial en SD WAN el plano de control es el encargado de proporcionar la inteligencia de la red mediante la recopilación de la información de enrutamiento proveniente de los equipos del plano de datos. Los datos de enrutamiento anunciados son conocidos como TLOC´s y hacen referencia a la combinación de un color, una encapsulación y un system ip que identifica de forma única al equipo que realiza el envío. Por otra parte los anuncios desde el plano de control hacia el plano de datos pueden ser influenciados por políticas centralizadas que a su vez se encargan de proporcionar un esquema lógico a la red, como puede ser full mesh o hub and spoke. Este enfoque permite la construcción de una red altamente escalable y la liberación de tareas a los equipos del plano de datos.

Otro beneficio de la separación del plano de datos es la tolerancia ante fallas ya que ante inconvenientes críticos el plano de datos puede seguir operando con normalidad hasta por 24 horas lo que da tiempo suficiente para aplicar una solución antes de que el usuario final pueda percibir la afectación del servicio.

3.3.1 Controladoras Vsmart

Los equipos vsmart son los encargados de realizar las funciones de control dentro de la red SD WAN mediante la redistribución de políticas e información de enrutamiento haciendo uso del protocolo OMP. Antes de empezar a compartir los anuncios las controladoras vsmart forman túneles DTLS/TLS contra las otras controladoras y contra los equipos del plano de datos que normalmente pueden ser equipos Vedge, Cedge o equipos ASR con una IOS de SD WAN. Posteriormente dentro de los túneles se establecen las sesiones OMP (peering) para enviar las notificaciones y mantener actualizada toda la red.

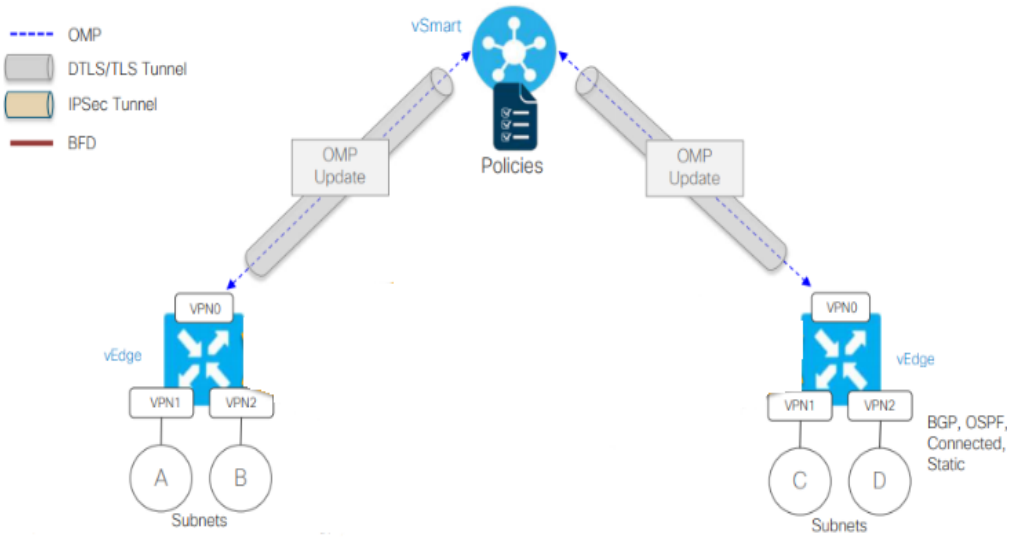


Figura 7.Actualizaciones desde el plano de control (Barozet, 2017).

Los equipos vsmart dentro de la arquitectura SD WAN realizan funciones similares a las efectuadas por los route reflector en redes basadas en BGP. Es decir, minimizan las sesiones de control en las topologías full mesh reduciendo de esta forma los recursos de maquina necesarios para establecer una topología de malla completa.

Los diseños de red para redes corporativas incluyen varias controladoras vsmart alojadas en puntos geográficamente distantes para garantizar un alto grado de redundancia y asegurar la continuidad de la operación ente la falla de algún equipo. Estas soluciones se pueden implementar on-premise o de manera hosteada, siendo esta ultima la más utilizada en la actualidad.

Las controladoras vsmart también son las encargadas de anunciar las políticas hacia los demás componentes de la red. Por otra parte, otra de las funciones que realizan estos equipos es la generación de certificados para autenticar a los equipos autorizados dentro de la red en producción.

3.4 Management plane (Plano de administración)

Continuando con la filosofía de separación de planos SD WAN proporciona una capa especializada para realizar las funciones de administración de los equipos alojados en la red diseñada bajo este esquema (conocida como fabric). Mediante

el uso el plano de administración se puede ejecutar o programar las tareas de una forma centralizada sin tener que intervenir equipos que se encuentren realizando funciones de envió de datos. La programación se realiza mediante funcionalidades de integración avanzadas a través de APIS y lenguajes de programación de alto nivel.

Este novedoso enfoque de administración de redes facilita de manera notable las actividades diarias de mantenimiento, así como el inventario y control de equipos que interactúan dentro del fabric para garantizar la comunicación de extremo a extremo. La gestión de la red a través del management plane no solo se encarga de realizar cambios en los equipos del plano de datos y el plano de control, sino que además está diseñado para recibir estadísticas de la red y generar graficas e informes sobre el comportamiento en tiempo real de los enlaces.

Otro factor importante al mantener una administración separada es la optimización de recursos tanto económicos como del personal encargado de las funciones de la operación de la red. Económicamente el beneficio se ve reflejado en los ahorros que se obtienen al no ser necesario el despliegue de una red dedicada para realizar monitoreo out band de los equipos o el uso de sistemas de gestión de terceros, mientras que la optimización del personal se da gracias a que se realizan procesos estandarizados de gestión y configuración aun cuando se cuente con diferentes tecnologías en el underlay.

Una falla en el management plane no altera ningún comportamiento de la red de producción por lo que se pueden programar actividades de optimización o mantenimiento sin afectar la operación normal de la red.

3.5 Plano de orquestacion (Orchestration plane).

Para entregar SD-WAN como un servicio utilizando la orquestación, un proveedor de servicios necesita una plataforma de orquestación SD-WAN para controlar y administrar el servicio. Esto generalmente implica una combinación de controlador SDN y software de virtualización de red que puede automatizar el aprovisionamiento y la operación del software y los elementos necesarios, muchos de los cuales se basarían en la nube(Craven, 2019).

El plano de orquestación es el encargado de proporcionar las funcionalidades de autenticación y control de acceso a los dispositivos que participan en la red SD WAN. Este control se realiza en base a listas blancas en donde se encuentra la

información de los equipos que pueden establecer conexiones hacia los demás equipos que hacen parte de los diferentes planos de esta arquitectura.

En las implementaciones de SD WAN es común encontrar el plano de control en ambientes cloud o bajo la administración del fabricante quien se encarga de alojar los equipos en sus data center de acuerdo a arquitecturas previamente diseñadas para garantizar altos niveles de disponibilidad.

El plano de orquestación está compuesto por uno o varios el equipo vBond los cuales por diseño se encuentran en zonas geográficas distantes y operan en modo activo – standby.

3.5.1 Equipo vbond

El vbond es el componente principal de la capa de orquestación, este ese encarga de recibir y verificar las solicitudes enviadas por los equipos que desean unirse al fabric de SD WAN. El Vbond previamente registra a los controladores vsmart y al vmanage para mantener información sobre sus direcciones ip y enviar esta información a los equipos que realicen el proceso de autenticación.

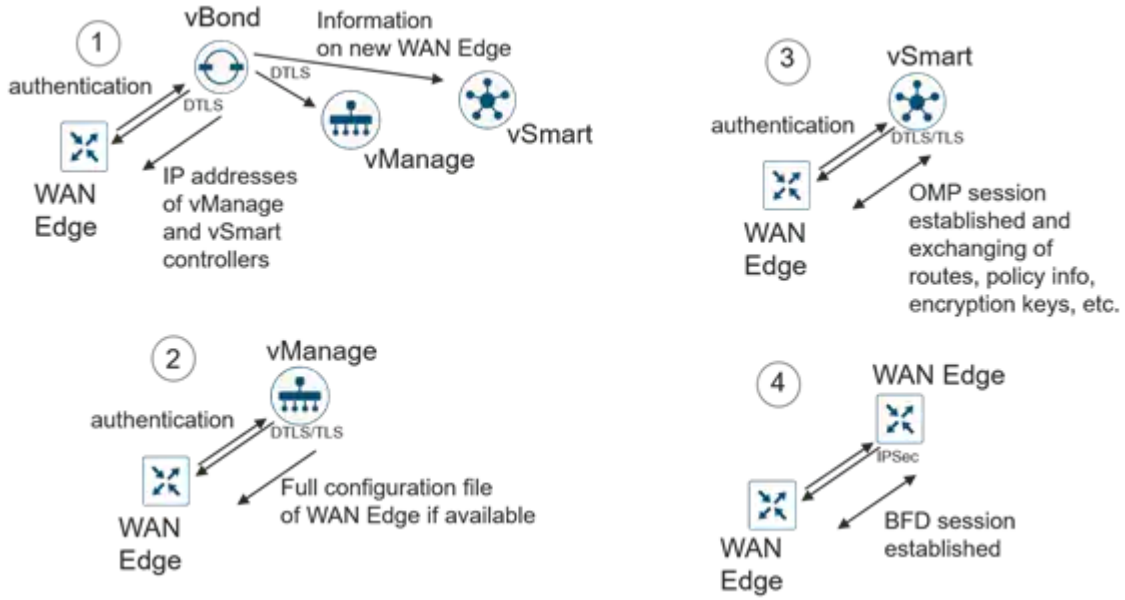


Figura 8. Funcionamiento del vBond (Cisco, 2020a)

Las funciones realizadas por el vbond se pueden observar en el siguiente paso a paso para la agregación de un nuevo equipo al fabric de SD WAN.

Como primer paso el equipo que quiere unirse a la red realiza un intento de autenticación con el vbond a través de un túnel DTLS. El Vbond utiliza un esquema de listas blancas para comprobar que el equipo que quiere conectarse a la red si es un equipo válido para así poderle enviar las direcciones ip de los controladores vsmart y del vmanage. Por otra parte, el vBond también informa a los controladores y al vmanage sobre el nuevo equipo que quiere unirse a la red.

En el siguiente paso el equipo inicia una sesión DTLS o TLS hacia los vsmart y el vmanage. Cuando se establece la sesión con el vmanage este le envía la configuración correspondiente a través de los vsmart. Así mismo, una vez se encuentren establecidas las sesiones contra los vsmart se levantarán las sesiones OMP para conocer la información de enrutamiento necesaria para realizar el envío de información en el plano de datos. Finalmente, con la información recibida el equipo establece a nivel del plano de datos las sesiones BFD por cada uno de los transportes haciendo uso del protocolo IP sec.

3.5.2 ZTP vs aprovisionamiento manual

Como método de autenticación hacia el vBond existen dos opciones que pueden ser utilizadas de acuerdo a las necesidades o capacidades de la red underlay.

El primer método es conocido como el ZTP (Zero Touch Privisioning) y consiste en una manera ágil de unir nuevos equipos en el dominio SD WAN. Este modelo requiere que el equipo sea conectado a una red con acceso a internet para que el equipo envíe automáticamente un query hacia el servidor ZTP de SD WAN. Este servidor enviara una respuesta con la información de su vBond asignado en donde puede realizar todo el proceso de autenticación y descubrimiento de los controladores, así como del vmanage para obtener su configuración.

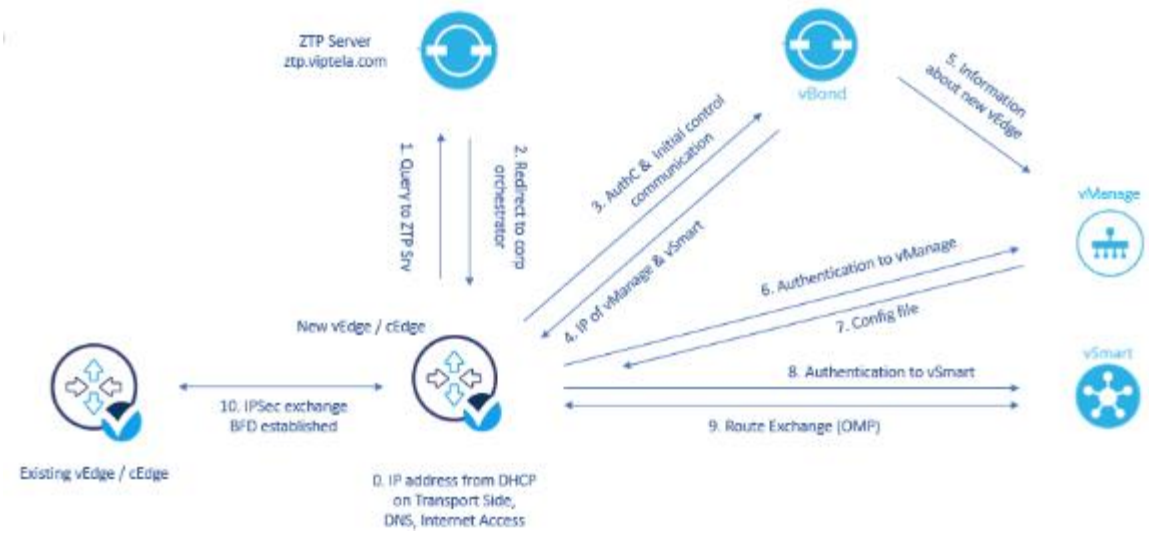


Figura 9. Funcionamiento de ZTP (Bialy, 2020)

Por otro lado, se encuentra la autenticación manual en donde es necesaria la configuración de la vpn de transporte para que se pueda establecer la comunicación con el vBond. Así mismo es necesaria la configuración de los parámetros system en donde se encuentran los dns, el system ip, el site id, la organización y la dirección pública del vBond.

Capítulo 4. Seguridad en redes SD WAN

El cuarto capítulo enmarca las funciones de seguridad implementadas dentro de las redes basadas en software para proteger de la información de usuario, así como la protección de la infraestructura sobre la cual se implementa la red.

4.1. Caracteristicas de seguridad en las redes basadas en software.

La seguridad se debe ser un aspecto crucial a la hora de desarrollar cualquier producto tecnológico ya que de no tomar las medidas adecuadas se puede abrir la posibilidad a ataques cibernéticos que pueden llevar a la suplantación de identidad y el posterior robo de información.

Los delitos informáticos presentan un crecimiento exponencial lo que ha generado preocupación no solo a los sectores especializados dedicados a la seguridad informática, sino que se ha convertido en una preocupación para cualquier usuario que haga uso de medios tecnológico.

Figura 10. Delitos informáticos en Colombia (Ceballos et al., 2019)

Estos antecedentes llevaron a diseñar estrategias de protección robustas e implícitas dentro de la filosofía de las redes basadas en software. Las innovaciones a nivel de seguridad se enfocan principalmente en dos aspectos; el primero de ellos es la seguridad que se debe proporcionar a los datos de usuario que son transportados a través de la red para evitar su alteración y garantizar la privacidad de la información. El segundo enfoque está dirigido a brindar protección a los componentes físicos y virtuales que hacen parte de este esquema de conexión.es decir, dar una respuesta oportuna ante ataques dirigidos a la infraestructura responsable de la lógica de conmutación de tráfico. Debido a lo anteriormente mencionado se hace énfasis en los niveles de seguridad que se encuentran integrados en el plano de control y en el plano de datos.

Los componentes de seguridad en SD WAN están basados en los siguientes preceptos.

Autenticación: Los esquemas de redes basadas en software permiten que solo los dispositivos debidamente autorizados puedan unirse a la red y puedan realizar envío y recepción de tráfico.

Encriptación: Las comunicaciones que se establecen entre los dispositivos son automáticamente aseguradas mediante el uso de protocolos de cifrado. Solo los dispositivos autorizados pueden cuentan con la información necesaria para descifrar y entender el mensaje.

Integridad: Las redes basadas en software utilizan mecanismos para garantizar que los mensajes no sean alterados cuanto hacen tránsito hacia su destino. En caso de que se detecte que algún paquete ha sido alterado, este es descartado inmediatamente.

Un beneficio de seguridad importante en los esquemas de interconexión basados en software es que no hace uso de servidores adicionales o infraestructuras alternas para proporcionar los niveles de seguridad. Esto hace que se generen beneficios económicos a las empresas que deciden optar por esta forma de interconexión.

4.2 Seguridad en el plano de control.

El plano de control de SD WAN hace uso de diferentes protocolos para asegurar el establecimiento de las sesiones de control bien sea entre controladoras vSmart o entre las controladoras y los equipos vEdge del plano de datos.

Cuando un nuevo dispositivo se une al fabric de SD WAN este crea un túnel provisional utilizando TLS o DTLS. Estos túneles se establecen contra los demás dispositivos y se consideran permanentes una vez se finalice satisfactoriamente el proceso de autenticación. El uso de estos protocolos de capa 4 otorgan privacidad a las comunicaciones y previenen la intercepción o manipulación de las conexiones por parte de componentes no autorizados. Estas características de DTLS /TLS son construidas en base al uso del algoritmo AES 256-GCM para proporcionar servicios de encriptación e integridad y los certificados digitales usados para los procesos de autenticación.

Las redes basadas en software SD WAN están capacitadas para hacer uso de estos protocolos de forma automática lo que aumenta los niveles de flexibilidad y escalabilidad de la solución.

4.2.1 Autenticación en el plano de contról

Dentro del proceso de autenticación en el plano de control los equipos hacen uso de certificados digitales con llaves de 2048 bits y el proceso de administración de este mecanismo es ejecutado mediante PKI (Public key infraestructure.) Para este proceso se cuenta con 3 componentes principales que son:

Llaves públicas: Estas llaves son generadas y compartidas con todos los destinatarios que requiera iniciar procesos de autenticación.

Llaves Privadas: Estas llaves permanecen dentro de los dispositivos y no son compartidas con los demás equipos.

Certificados: Estos certificados son firmados por una autoridad certificadora. La autoridad certificadora se encarga de garantizar que el dispositivo es quien dice ser.

Debido a que las controladoras vSmart pertenecientes al plano de control requieren establecer sesiones de control con los equipos del plano de datos, estos también están en capacidad de manejar los mecanismos de autenticación por medio de PKI. En los equipos del plano de datos las claves tanto públicas como privadas se encuentran en un chip instalado de fábrica, mientras que en las controladoras estas claves y certificados son administrados manualmente.

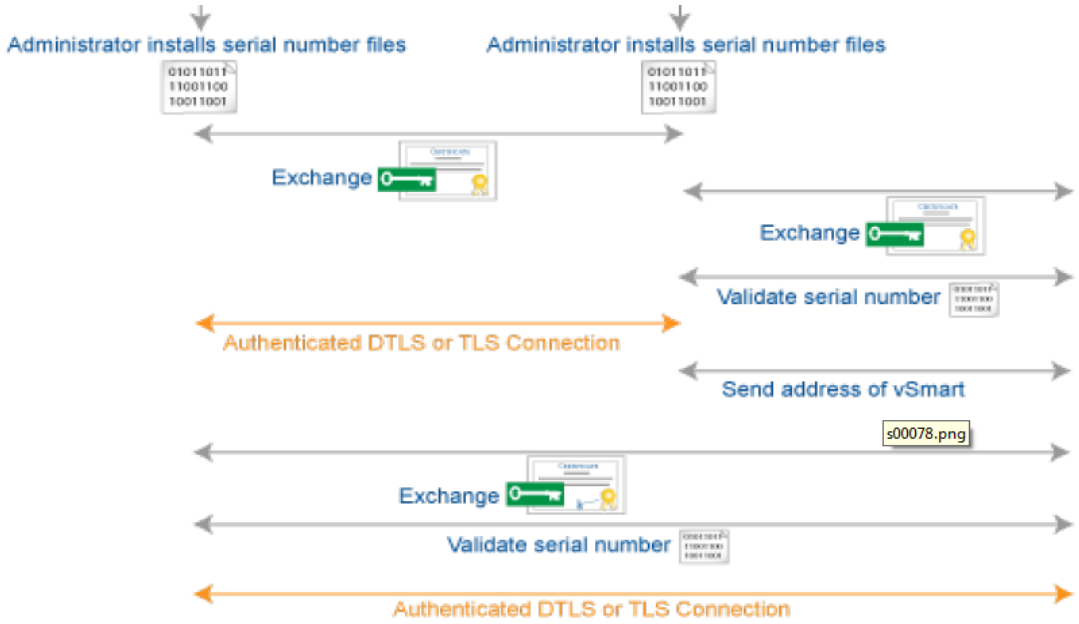


Figura 11. Autenticación en el plano de control (Cisco, 2019)

El proceso de autenticación en este plano inicia cuando los equipos que quieren hacer parte del fabric de SD WAN contactan al dispositivo vBond encargado de la capa de orquestación quien se encarga de realizar la validación en base a listas blancas para autorizar o denegar el acceso al equipo. Si el proceso de verificación en las listas blancas es exitoso los dispositivos establecen túneles TLS o DTLS entre ellos e inician el proceso de autenticación mediante el intercambio de llaves públicas y certificados digitales.

4.2.2 Encriptación en el plano de control

El proceso de encriptación en plano de control se lleva a cabo mediante el uso de los protocolos transport layer security (TLS) y datagram transport security DTLS. Estos protocolos se encargan de cifrar el tráfico mediante el uso de criptografía asimétrica para realizar el intercambio de llaves durante el proceso de establecimiento de las sesiones DTLS/TLS. La diferencia fundamental entre estos dos protocolos es que TLS hace uso de TCP mientras que DTLS ha sido diseñado para ser usado sobre el protocolo UDP.

Para iniciar su funcionamiento estos dos protocolos en su fase inicial negocian los parámetros que van a permitir dar la protección a la información compartida a través de la sesión. Este proceso es conocido como hanshake.

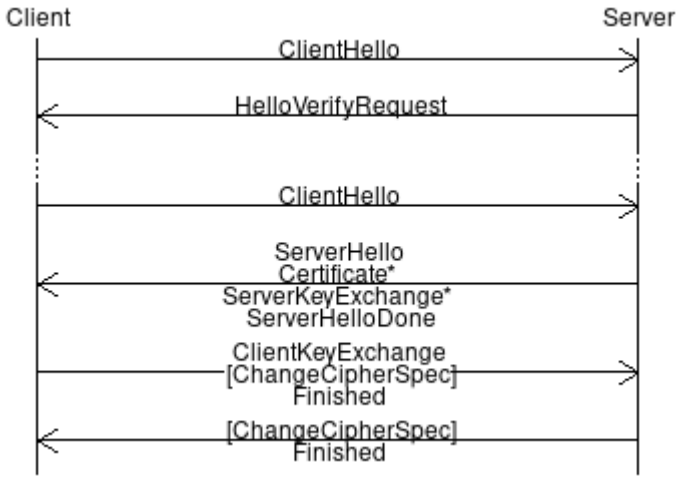


Figura 12. Hanshake DTLS (Ueno, 2020).

Para el caso de las redes SD WAN los equipos del plano de control solo habilitan el proceso de comunicación TLS/DTLS hacia los equipos previamente autorizados por equipo vBond que se encuentra en el plano de orquestación, proporcionando de esta forma un nivel de seguridad adicional al establecimiento de las sesiones.

4.2.3 Integridad en el plano de contról

Para garantizar que los paquetes enviados a través de la red SD WAN no se han alterado en el transcurso de su camino, es necesario el uso de protocolos que garanticen la integridad de la información enviada desde el origen al destino. SD WAN hace uso de dos mecanismos para garantizar esta integridad, el primero de ellos es el uso de algoritmos hash como son sha1 y sha2. Estos algoritmos de una sola vía generan un hash en base a la información contenida y adjuntan el resultado al paquete que es enviado a su destinatario.

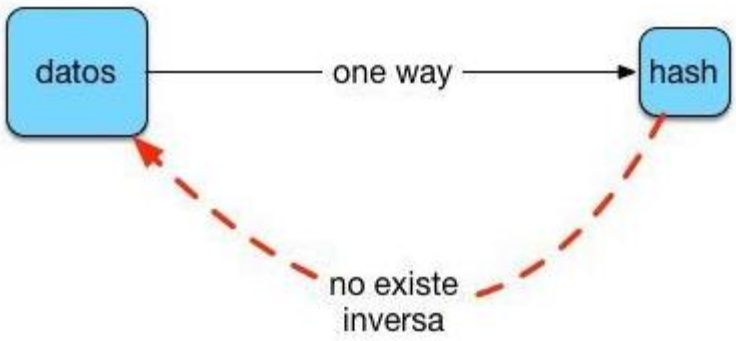


Figura 13. Algoritmo de una sola vía (Álvarez, 2016).

En el destino se ejecuta el mismo algoritmo para verificar nuevamente el valor del hash. En el caso que el resultado sea diferente al enviado por el emisor, el paquete es descartado ya que indica se ha realizado una modificación en el camino y por lo tanto no corresponde con la información originalmente enviada. Por otra parte, se realiza el uso de claves públicas y privadas en donde el equipo emisor envía un reto hacia el equipo destino para que lo encripte haciendo uso de su clave privada. Cuando el reto es regresado al equipo emisor este utiliza su clave publica para verificar el paquete corresponde al inicialmente enviado.

4.3 Seguridad en el plano de datos

Las redes basadas en software SD WAN tienen una gran ventaja con respecto a las redes tradicionales ya que aplican mecanismos de seguridad automáticos para proteger los datos enviados entre los dispositivos en el plano de datos. En las redes tradicionales se pueden configurar políticas para proteger el forwarding plane, pero esto representa una mayor inversión en tecnologías de seguridad y en la infraestructura necesaria para administrar estas características.

Por el contrario, las redes basadas en software permiten una administración convergente y fácilmente gestionable de los protocolos que realizan tareas específicas de seguridad en el plano de datos. Estos protocolos garantizan las funciones de autenticación, encriptación e integridad de la información entre el emisor y el receptor de los mensajes.

La base fundamental a nivel de seguridad en el plano de datos está conformada por la creación dinámica de túneles Ip Sec entre los dispositivos involucrados en

reenvío de datos. Al igual que en el plano de control, esta creación de túneles solo se realiza entre equipos previamente autenticados en el Vbond que se encuentra ubicado en el plano de orquestación. De acuerdo con (Bustos, 2019) las principales características de Ip Sec son las siguientes : .

- Confidencialidad, al utilizar algoritmos para cifrar la información antes de ser transmitida.
- Integridad, garantiza que la información no sea alterada durante la transmisión.
- Autenticación, verifica la identidad del origen y confiabilidad de los datos

Como se mencionó con anterioridad, la configuración de los túneles ip sec se realiza de forma automática entre los equipos autorizados, sin embargo, SD WAN permite la configuración manual de parámetros para modificar atributos de las conexiones o incluso definir la creación por defecto de túneles genéricos de enrutamiento (GRE).

4.3.1 Autenticación en el plano de datos.

A diferencia de las redes tradicionales en el plano de datos de SD WAN no se hace uso del protocolo de intercambio de claves IKE ya que el diseño de esta nueva arquitectura permite el aseguramiento del canal mediante las funciones ejecutadas por DTLS/TLS en el plano de control. Esto lleva a que el plano de datos pueda establecer las asociaciones de seguridad de una forma más eficiente evitando el uso de recursos para el manejo de claves. Sin embargo, existen otros dos protocolos inmersos dentro de ipsec que realizan funciones de autenticación como lo son el encapsulation security payload (ESP) y el Autentication header (AH). ESP puede ser usado para proporcionar confidencialidad, autenticación de los datos origen, integridad y servicios anti replay. Los servicios proporcionados dependen de las opciones seleccionadas durante el establecimiento de las security associations (Kent, 2005).

4.3.2 Encripcion en el plano de datos.

La encriptación en el plano de datos es realizada mediante el uso del algoritmo simétrico AES-256. Este algoritmo hace uso de la misma clave para cifrar o

descifrar la información entre los diferentes nodos de la red. Para el caso de SD WAN cada dispositivo del plano de datos se encarga de generar y compartir sus propias llaves hacia las controladoras vsmart quienes son las encargadas de distribuirlas hacia los demás equipos teniendo en cuenta las políticas de control establecidas.

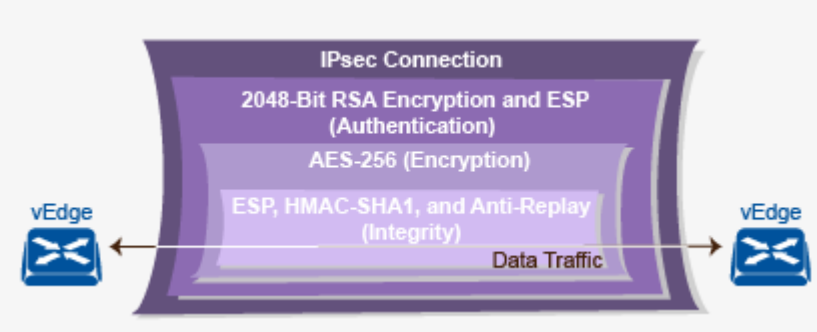


Figura 14. Seguridad en el plano de datos (Cisco, 2020a)

Aunque la generación de las claves por parte de equipos es un proceso automático, este comportamiento puede ser modificado mediante modificación de los parámetros relacionados con el algoritmo de cifrado.

4.3.3 Integridad en el plano de datos.

Las características de integridad en el plan de datos se lleva a cabo a través de los protocolo Encapsulation security payload (ESP) , authentication Header (AH) Y anti replay. ESP se encarga de proteger la integridad de la información a través de mecanismos de encriptación y la generación de un checksum que se adjunta al paquete. Por otro lado, HA ofrece características de integridad mediante el proceso de autenticación. A diferencia de ESP que genera el checksum solo en base al payload y los encabezados ip internos HA realiza el cálculo del checksum en base a todos los campos en el paquete. Por último, se encuentra el mecanismo de anti replay que consiste en el uso de dos mecanismos para evitar ataques de man in the midle. El primer mecanismo de anti replay es el uso de un numero de secuencia que es insertado por el equipo que genera la información, así en caso al destino llegue un paquete que no corresponde a la secuencia esperada este es descartado de inmediato. El segundo mecanismo consiste en la creación de una ventana en donde se define un rango fijo de secuencias dentro de las cuales deben estar los paquetes recibidos.

Capítulo 5. Separación de planos en SD WAN

El quinto capítulo presentará los beneficios de la separación de planos en redes SD WAN, así como las mejoras que esto trae en el momento de realizar el diseño de una red escalable. La flexibilidad y escalabilidad de las redes corporativas son puntos neurálgicos en las políticas de TI por lo tanto las nuevas arquitecturas de red hacen énfasis en estos aspectos.

5.1. Separación de los planos de control y de datos

Los esfuerzos de los sectores académicos y las grandes entidades de comunicaciones por dotar a las redes características programables que se adapten a cualquier tráfico llevo a que desde la década de 1990 se iniciaran investigaciones para dar un salto evolutivo en este campo. Con el crecimiento del tráfico y la necesidad por parte de los operadores de proporcionar mejores niveles de calidad se enfocaron los esfuerzos en la mejora de la ingeniería de tráfico mediante la creación de estándares abiertos y la creación de mecanismos de reenvío de tráfico basado en hardware.

Los intentos iniciales de separar los planos de control y de datos fueron relativamente pragmáticos, pero representaron una desviación conceptual significativa del acoplamiento convencionalmente estrecho de Internet. Los esfuerzos para separar el control de la red y el plano de datos resultaron en varios conceptos que se han llevado adelante en diseños SDN posteriores (Feamster et al., 2014). El desarrollo de nuevos protocolos, así como la creación de API´s llevaron a que las redes basadas en software se convirtieran en un nuevo paradigma que ofrece capacidades mejoradas con respecto a las redes tradicionales.

5.2. Ventajas de la separacion de planos

Las redes basadas en software y en particular las redes basadas en software para interconexión SD WAN potencian sus funciones y capacidades gracias al desacoplamiento de funciones en planos separados. Cada uno de ellos se encarga de realizar funciones específicas dentro del proceso de comunicación, brindando así la flexibilidad necesaria para proporcionar los niveles de calidad requeridos por cada aplicación o servicio.

Aunque para muchas empresas la separación de planos pasa inadvertida a la hora de seleccionar la mejor opción de conectividad en su entorno corporativo, es

un aspecto que potencia de forma sustancial las capacidades de la red y el tráfico de aplicaciones en la nube. A continuación, se relacionan las ventajas que proporciona esta separación de funciones.

- Minimiza las sesiones de control

Una de las ventajas de la separación de planos es la reducción de sesiones de control entre los equipos del plano de control y del plano de datos. En este caso los controladores actúan de una forma similar a los route-reflector de las redes basadas en BGP para servir como espejo de las sesiones de control y evitar que los equipos del plano de datos tengan que establecer sesiones de control contra todos los demás equipos.

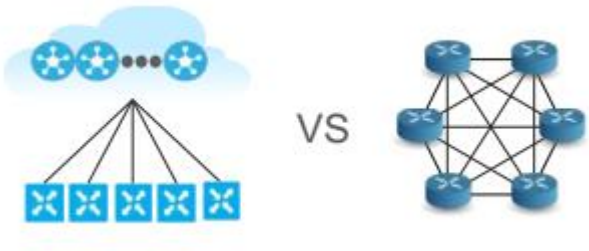


Figura 15. Sesiones de control con separación de planos (Barozet, 2017)

- Mejora los niveles de escalabilidad

La escalabilidad es un aspecto clave en las redes modernas ya que el aumento de tráfico y la creación de nuevas y sofisticadas aplicaciones requiere de un mecanismo de conexión que pueda crecer y adaptarse de forma rápida a los cambios. Desde el punto de las redes basadas en software SD WAN, los niveles de escalabilidad son altos debido a que el plano de datos puede crecer exponencialmente sin tener que modificar los equipos y las funciones encargadas de realizar las funciones de control.

Múltiples equipos encargados del reenvío de datos pueden estar controlados por un solo componente que puede estar virtualizado o configurado en la nube, lo que facilita el despliegue de la red de una forma organizada y menos costosa en comparación a las redes tradicionales.

- Programación de la red

Las redes SD WAN puede ser programadas para realizar acciones en base a eventos ocurridos en la red. El caso más común es la configuración del protocolo DPI (Deep packet inspection) para verificar el contenido del paquete y en base a ello aplicar políticas de app aware routing basadas en parámetros configurados para cada tipo de tráfico. Otro aspecto importante de la programabilidad de la red es la capacidad de usar API´s para programar comportamientos avanzados en base a lenguajes de programación de alto nivel.

- Administración centralizada y actualización de equipos

Las funciones de administración pueden ser ejecutadas sin la necesidad de afectar las funciones de reenvío de tráfico. Esto se da gracias a las políticas centralizadas desplegadas desde el plano de control. Estas políticas pueden crear redes lógicas haciendo filtrado de los anuncios enviados a los equipos del plano de datos.

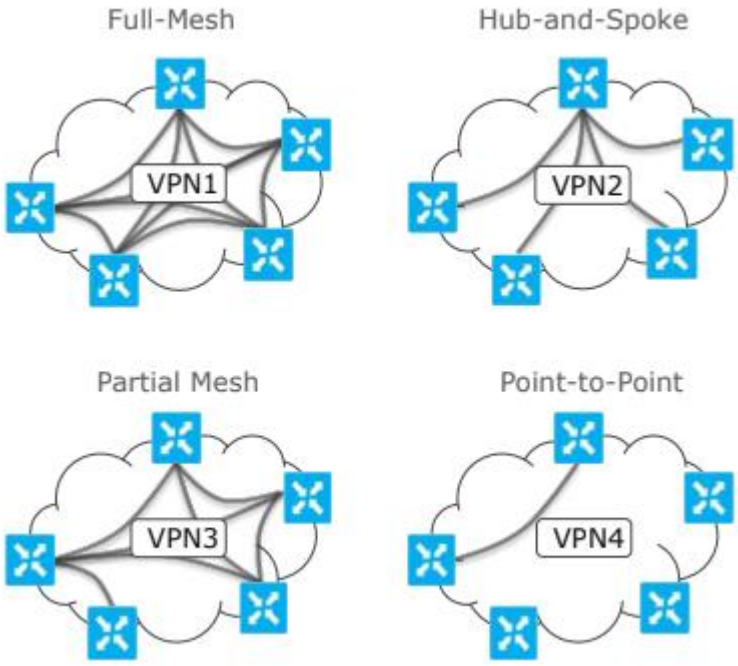


Figura 16. Topologías lógicas mediante políticas centralizadas (Barozet, 2017)

A diferencia de las redes tradicionales en donde en la mayoría de los casos la actualización de equipo se debe hacer de forma manual en cada uno de ellos SD

WAN permite la actualización masiva de equipos mediante las funciones incorporadas en el plano de administración.

- Optimización de costos

El despliegue de una red SD WAN representa un ahorro significativo en los costos asociados al mantenimiento y administración de la red. Así mismo al tratarse una red overlay capaz de ejecutarse cobre cualquier tecnología de transporte no está limitada por capas subyacentes que representen altos costos para la organización.

Capítulo 6. Plataforma de administración y rol de las redes de transporte

En este capítulo se da a conocer el rol que desempeñan las diferentes tecnologías de transporte que sirven como red underlay para el despliegue de redes basadas en software como SD WAN. Estas redes se encargan de proporcionar servicios de conectividad de extremo a extremo para facilitar la comunicación entre los diferentes nodos de la red.

6.1 El vmanage y sus caracteristicas

El componente diseñado para realizar las tareas de la capa de gestión es conocido como el vmanage. Este componente es accesible a través de un dashboard que consiste en una interfaz gráfica que facilita la interacción y la administración de la red de una forma práctica y simplificada. Las configuraciones realizadas pasan por un proceso previo de verificación antes de ser propagadas hacia los equipos finales a través de las sesiones de control previamente establecidas.

Uno de los aspectos relevantes en este modelo de configuración es el uso de protocolos especializados en la configuración de redes diseñadas para la automatización. En el caso de SD WAN los protocolos utilizados para realizar la configuración son el Netconf y Restconf.

El protocolo NETCONF se basa en la llamada a procedimiento remoto (RPC), un protocolo cliente / servidor que permite que un programa solicite un servicio de otro programa sin tener que comprender los detalles de la red. NETCOF fue diseñado para compensar las deficiencias del Protocolo simple de administración de redes (SNMP) y los protocolos de interfaz de línea de comandos (CLI) que se aplican a la configuración de los dispositivos de red (Rouse, 2013) .

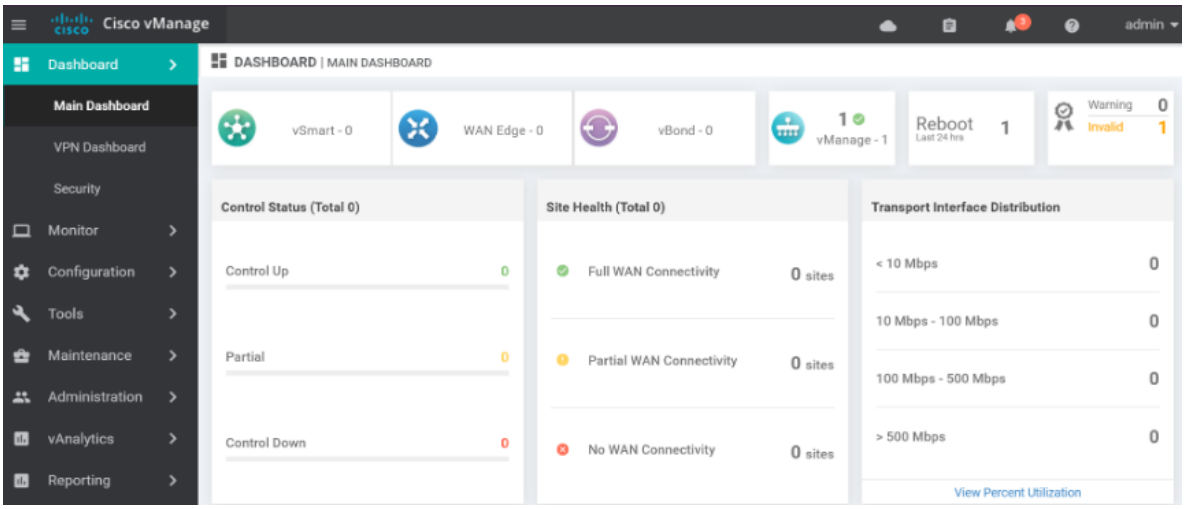


Figura 17. Pantalla Inicial Dashboard (Autor, 2021)

Los equipos del fabric de SD WAN tienen la capacidad de operar en dos modos; el primero de ellos es el modo CLI en el cual se pueden realizar las configuraciones de forma tradicional, es decir se puede realizar directamente la configuración sobre el equipo. Por otro lado, está el modo "vmanage "en donde los equipos se mantienen bajo el dominio del vmanage y la configuración se realiza exclusivamente a través del dashboard.

Teniendo en cuenta que en la mayoría de los escenarios el vmanage se encuentra en la nube del fabricante, es común que se establezcan políticas de control de acceso para permitir el ingreso al dashboard solo a través de las ip públicas autorizadas. Esto sumado a la capacidad de crear usuarios con diferentes roles da un grado de seguridad adicional a la gestión de la red.

6.2 Funcionalidades generales del vmanage

El vmanage cuenta con diferentes módulos que permiten cubrir un amplio rango de funcionalidades no solo a nivel de configuración sino también las relacionadas con el monitoreo del comportamiento de la red. A continuación de relaciona algunas de las funcionalidades de cada módulo.

6.2.1 Módulo de dashboard

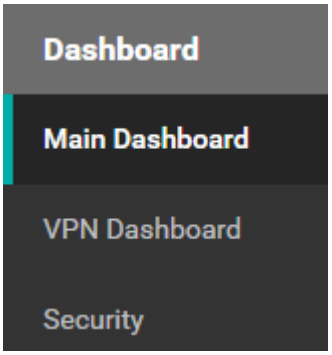


Figura 18. Módulo dashboard (Autor, 2021)

Este módulo se puede considerar como el enlace de inicio del entorno web del vmanage. Adicionalmente se pueden realizar configuraciones asociadas al comportamiento del entorno de gestión.

6.2.2 Módulo de monitoreo

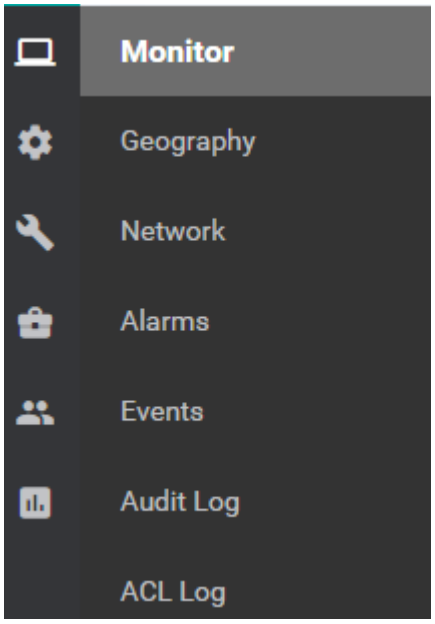


Figura 19. Módulo Monitor (Autor, 2021)

El módulo monitor comprende las opciones más relevantes para realizar un seguimiento adecuado de los servicios configurados. En esta opción se puede observar el performance de los canales, así como su ubicación geográfica mediante el esquema de coordenadas. Los eventos generados sobre la red y los logs generados por dichos eventos también son visibles a través de esta opción.

6.2.3 Módulo de configuración

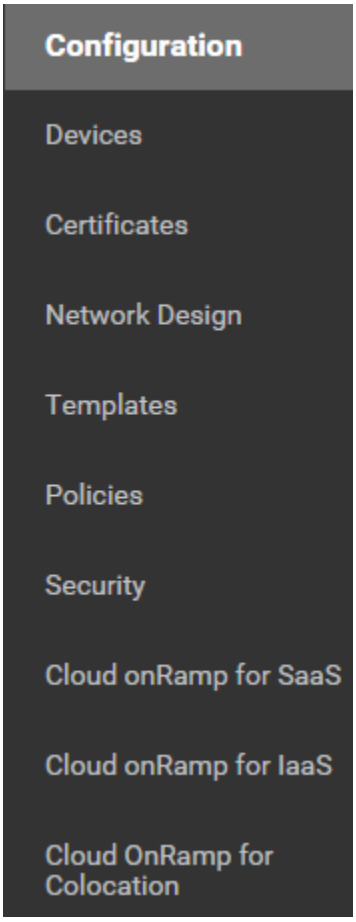


Figura 20. Módulo de configuración (Autor, 2021)

Todos los equipos que componen el fabric de SD WAN son configurables a través de la asignación de plantillas (templates) o a través de la configuración de políticas centralizadas o localizadas. El módulo de configuración permite el ingreso

a los dispositivos y a los template disponibles para asignar la configuración. En este módulo también se encuentran opciones de seguridad como la verificación de certificados, además de la opción para configurar parámetros de calidad de servicio a través de políticas.

6.2.4 Módulo de herramientas

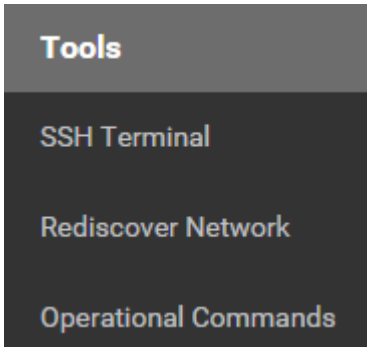


Figura 21. Modulo Tools (Autor, 2021)

Aunque la filosofía de SD WAN consiste en realizar a la configuración a través del entorno web, también se puede establecer acceso hacia los equipos a través de un terminal SSH configurado en el módulo de herramientas. En el submenú también se encuentran disponibles las opciones para forzar el descubrimiento de la red y la opción para obtener estadísticas útiles para la resolución de problemas por ejemplo el tech support de los equipos.

6.2.5 Módulo de administracion

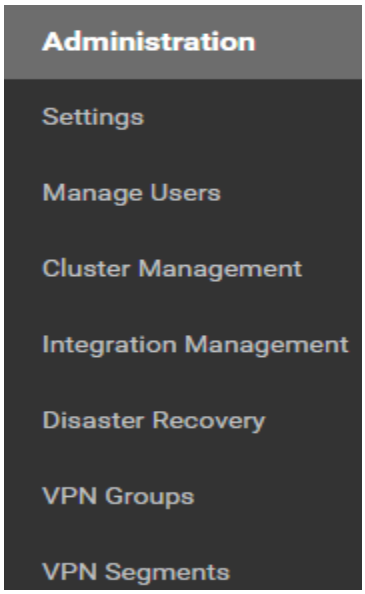


Figura 22.Módulo de administración (Autor, 2021)

El módulo de administración del entorno grafico permite la modificación de parámetros a nivel de servidor y la administración de usuarios. En esta opción se puede modificar a capacidad de almacenamiento para la generación de gráficas y parámetros adicionales relacionados con redundancia del servidor que aloja la aplicación web.

6.2.6 Módulo de análisis

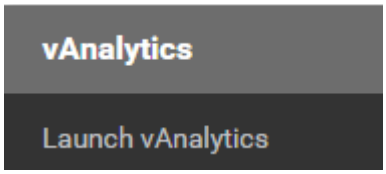


Figura 23. Módulo de Análisis (Autor, 2021)

El módulo de análisis permite observar el comportamiento de los canales, así como de las aplicaciones que cursan la red. Esta opción permite observar estadísticas de jitter, latencia, y perdida de paquetes, así como las

correspondientes graficas que permiten realizar un análisis dinámico del comportamiento del fabric.

6.3 Redes de transporte y plataforma de administración

Los esquemas de conexión wan mediante arquitecturas de redes basadas en software integran las diferentes tecnologías mediante el uso de la interface grafica de administración. Esta característica facilita el despliegue de redes de área amplía haciendo uso de la infraestructura que ya se encuentra desplegada. Al tratarse de redes overlay, las redes basadas en software gestionan de manera estandarizada las conexiones establecidas a través de los diferentes transportes.

En la terminología de las redes basadas en software SD WAN cada uno de los transportes son conocidos como colores y deben ser asociados a la VPN 0 la cual es usada para gestionar las conexiones de transporte entre los diferentes nodos.

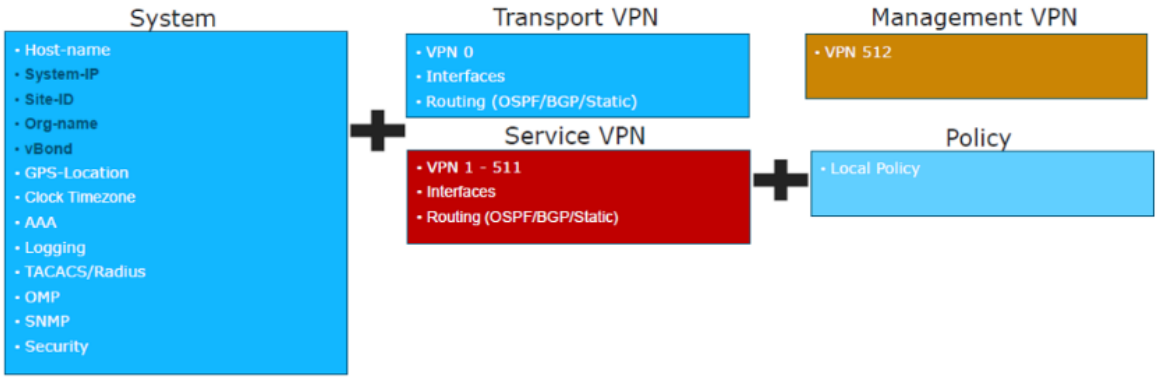


Figura 24. Segmentación de vpn´s (Dclessons, 2020)

El uso de transportes asociados a colores proporciona una mejora notable en cuanto a flexibilidad ya que las políticas configuradas en el plano de control pueden ser aplicadas a colores específicos.

En los entornos de producción cada vez más se está haciendo uso de enlaces de internet como medio de transporte debido a su bajo costo con relación a otras tecnologías.

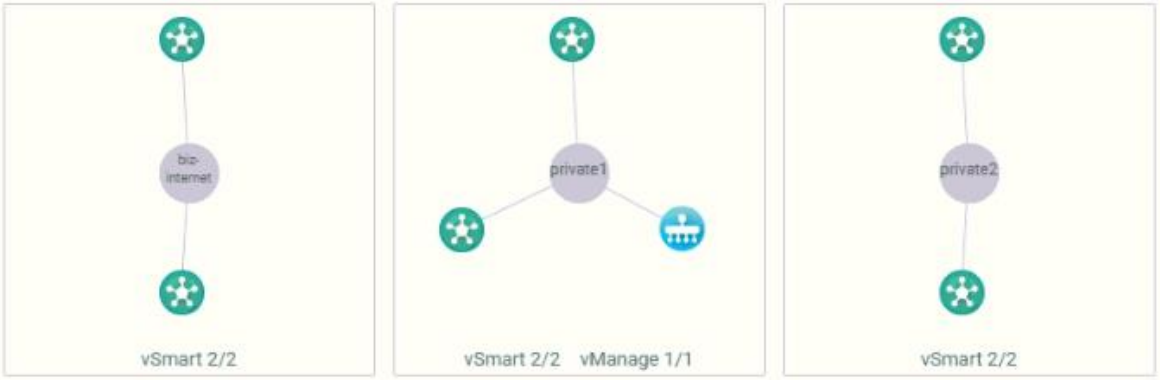


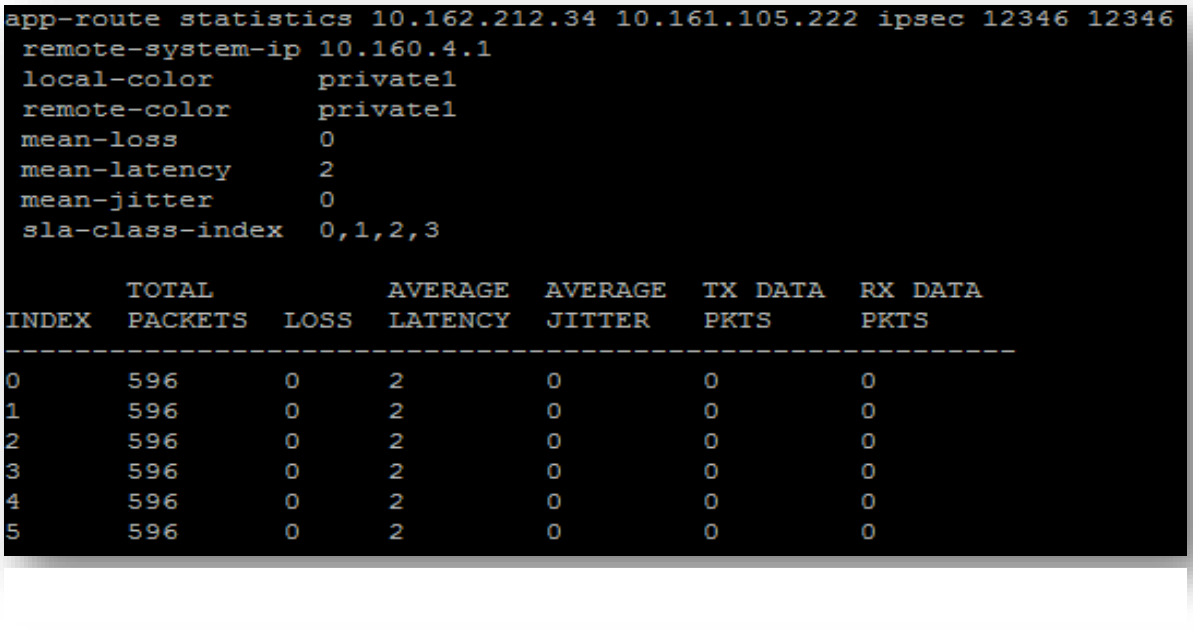
Figura 25. Esquema de colores en SD WAN (Autor)

Desde la plataforma de administración vmanage es posible realizar la configuración de políticas asociadas a las vpn para determinar el comportamiento del tráfico sobre la red overlay. Este comportamiento es el mismo sin importar la tecnología de trasporte o red underlay que se esté utilizando.

Las implementaciones de SD WAN por defecto realizan el balanceo de cargas entre los diferentes colores disponibles para alcanzar el TLOC destino. Este comportamiento puede ser modificado desde el entorno de administración mediante la configuración de políticas en base a protocolos de redundancia de primer salto como vrrp o a través de políticas basadas en aplicación en las cuales se puede asignar el color por el cual debe ser enviado el tráfico.

6.4 Monitoreo de estadísticas y toma de decisiones.

Si bien cada uno de los transportes o colores proporciona unas garantías de calidad de servicio específicas, SD WAN hace uso de su plataforma de administración integrada para mantener el control de estadísticas de cada canal y realizar cambios en la dinámica del tráfico. Las estadísticas de jitter, latencia, perdida de paquetes son recopiladas en cada uno de los equipos que intervienen dentro del fabric de SD WAN y pueden ser usadas en conjunto con protocolos de inspección de paquetes como DPI para dar granularidad al tráfico enviado entre los diferentes nodos que componen la red.



```
app-route statistics 10.162.212.34 10.161.105.222 ipsec 12346 12346
 remote-system-ip 10.160.4.1
 local-color      private1
 remote-color     private1
 mean-loss        0
 mean-latency     2
 mean-jitter      0
 sla-class-index  0,1,2,3

       TOTAL          AVERAGE  AVERAGE  TX DATA  RX DATA
INDEX  PACKETS  LOSS  LATENCY  JITTER   PKTS     PKTS
-------------------------------------------------------
0      596      0     2        0        0        0
1      596      0     2        0        0        0
2      596      0     2        0        0        0
3      596      0     2        0        0        0
4      596      0     2        0        0        0
5      596      0     2        0        0        0
```

Figura 26. Generación de estadísticas de transporte (Autor, 2021)

Las estadísticas generadas por los equipos del plano de transporte son enviadas al plano de administración, más específicamente hacia el equipo vmanage que se encargada de generar informes estadísticos en base a la información recibida. Posteriormente desde el plano de administración se realiza la configuración de las políticas de control de tráfico para influenciar el comportamiento de la red en base a la calidad de los enlaces activos. La configuración de las políticas de tráfico debe seguir una secuencia lógica consistente en:

1. Creación de policy list.
2. Configure Traffic Rules
3. Asociar las políticas a los sitios y a las vpn´s
4. Activación de la política

Esta secuencia puede ser realizada a través de la interface grafica del vmanage o a través de la configuración por CLI. La configuración de las políticas se encuentra fuera de los objetivos del presente documento.

6.5 Redundancia a nivel de transporte

La redundancia a nivel de transporte comprende la creación de un diseño de red que haga uso de las diferentes alternativas de conexión ofrecidas por los diferentes colores (transportes) en la en la red. Un adecuado diseño debe permitir la continuidad operativa de la red mediante configuraciones lógicas en los equipos involucrados, así como de conexiones físicas para permitir alternativas en la salida y el ingreso de tráfico.

Los dos esquemas principales de redundancia a nivel de transporte son la redundancia por mallado y la redundancia basada en tloc extensión.

6.5.1 Redundancia mediante mallado (MESH)

En este esquema de redundancia los router son conectados a todos los transportes disponibles manteniendo la disponibilidad del tráfico a través de los equipos de respaldo.

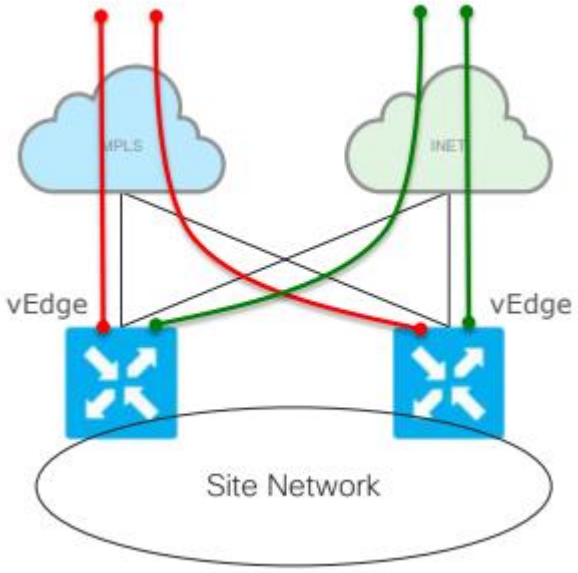


Figura 27. Transport mesh (Barozet, 2017)

Cuando un transporte presenta una caída los equipos detectan esa condición y dan por caídos los túneles. Esto hace que los prefijos sigan siendo alcanzables a través del mismo color que se encuentra asociado al equipo de respaldo.

6.5.2 Redundancia mediante tloc extensions.

El esquema de redundancia a través de TLOCS extensions hace uso de conexiones entre equipos formando un peering que sirve como mecanismo de redundancia para alcanzar los transportes asociados al equipo de respaldo. Los túneles pueden ser establecidos a través de los transportes conectados directamente, así como a través de los tloc extensión entre los equipos.

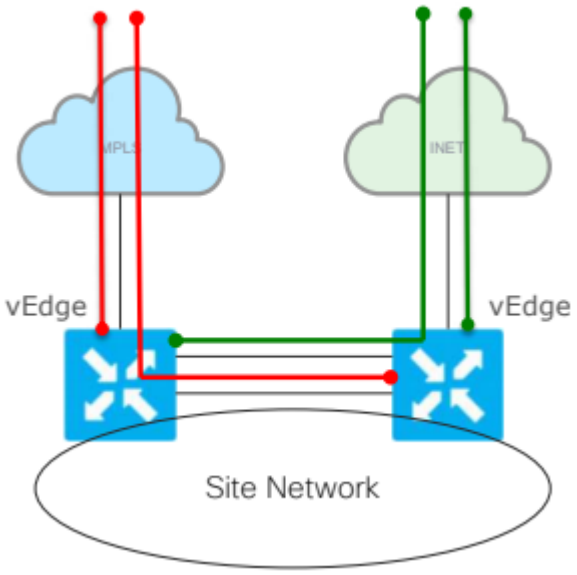


Figura 28. Redundancia mediante TLOCS extensions (Barozet, 2017)

En este se utilizan vlan independientes para para establecer la comunicación entre equipos y crear el tloc extensión. Si un equipo es inaccesible el otro equipo tomara las funciones de envío y recepción de tráfico a través de los transportes que sean alcanzables en ese momento.

Capítulo 7. Implementación de una red SD WAN en un ambiente de producción.

En este capítulo final se realiza la documentación de los procedimientos necesarios para realizar la implementación de una red basada en software SD WAN en un ambiente de producción. En este capítulo se describen los requerimientos de diseño y técnicos necesarios para el despliegue de este tipo de redes.

7.1 Planteamiento del escenario.

Con el propósito de realizar la transferencia de conocimientos adquiridos se plantea un escenario de red SD WAN simplificado en donde se documenta el paso a paso para realizar la configuración de este tipo de redes. Por lo tanto, se plantea un escenario de red con 3 sedes remotas y un data center centralizado los cuales tendrán una configuración en HA mediante el uso de dos equipos viptela vedge 1000 para las sedes y equipos ASR1001-X para el data center. Como red underlay se hará uso de canales MPLS y canales de internet. La distribución física de las sedes se plantea de la siguiente forma.

	Ciudad	Equipo 1	Equipo 2
Sede 1	Cali	Vedge 1000	Vedge 1000
Sede 2	Medellín	Vedge 1000	Vedge 1000
Sede 3	Barranquilla	Vedge 1000	Vedge 1000
Data center	Bogotá	ASR1001-X	ASR1001-X

Tabla 1. Distribución de ciudades

7.2 Consideraciones de diseño

Teniendo en duenta la arquitectura propuesta se requiere definir los los site id que identifian cada una de las sedes y los system ip que hacen referencia a cada uno de los equipos involucrados en la solución. Asi mismo se deben tener presentes las vpn de servicio por donde se enviara el trafico de extremo a extremos.

Ciudad	Site id	System ip
Cali	31	10.160.0.31
Medellín	43	10.160.0.43
Barranquilla	50	10.160.0.50
Bogotá	1001	10.160.4.1

Tabla 2. Site id y system ip

En el escenario planteado se van a ahacer uso de 3 VPN´s de servicios las cuales van a estar identificadas como VPN 501, VPN 502 y VPN 503.

Como protocolo de redundancia de primer salto se va a hacer uso de VRRP para proporcionar el balanceo entre los equipos y canales configurados en cada sede. A continuación se representa la conectividad entre una de las sedes y el data center.

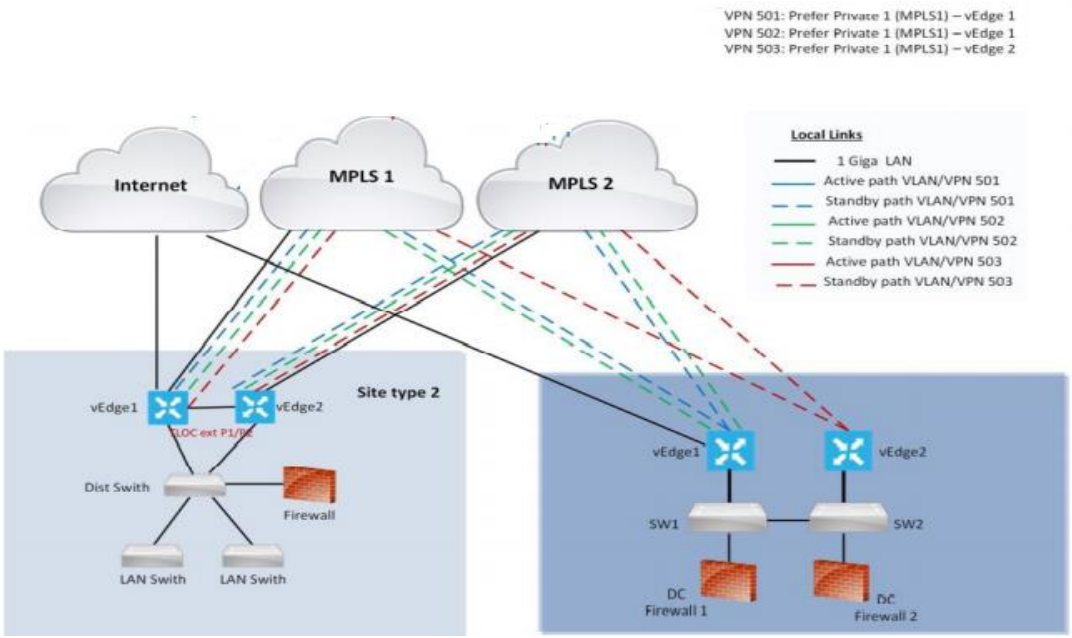


Figura 29. Conectividad entre sede y DC (Autor,2021)

Desde el plano de trasporte para las sedes se hace uso de la red MPLS la cual será dividida en dos colores: MPLS y MPLS 2 a su vez se hará uso de un canal de internet dedicado conectado únicamente al equipo 1 de cada sede. Para los equipos ubicados en el data center la conexión a internet estará conectada tanto al equipo 1 como al equipo 2.

7.2.1 Diseño del direccionamiento

Teniendo en cuenta que se utilizaran 3 VPN´s se realiza la asignación de direccionamiento de la siguiente forma:

Ciudad	VPN1	VPN3	VPN3
Cali	172.51.11.0/29	172.52.11.0/29	172.53.11.0/29
Medellín	172.51.32.0/29	172.52.32.0/29	172.53.32.0/29
Barranquilla	172.51.12.0/29	172.52.12.0/29	172.53.12.0/29
Bogotá	10.50.40.8/29	10.50.40.16/29	10.50.40.24/29

Tabla 3. Direccionamiento LAN

Para efectos de interconexión entre los diferentes sitios es necesario establecer el direccionamiento WAN y el direccionamiento público de internet del que se va a hacer uso.

Ciudad	Direccionamiento público	WAN 1 / WAN 2
Cali	190.85.252.96/29	10.162.41.118/30 - 10.162.41.34/30
Medellín	181.49.11.56/29	10.164.48.238/30 - 10.164.49.190/30
Barranquilla	190.85.252.168/29	10.168.31.42/30 - 10.168.31.246/30
Bogotá	181.57.128.226/30	10.161.105.206/30 - 10.161.105.222/30

Tabla 4. Direccionamiento WAN e internet

7.2.3 Controladores y equipo vbond

Las funciones de orquestación y de control en nuestro escenario, se realizarán por medio de un equipo vedge cloud que realizara las funciones de Vbond y por dos equipos Vsmart que realizarán las funciones del plano de control.

Debido a que el equipo vbond es un equipo virtualizado que proporciona el vendor a la hora de adquirir los servicios; no se profundizara en la configuración de este equipo.

7.3 Configuración de la solución SD WAN para un entorno corporativo

Para que se pueda hacer uso de equipos en la red sd wan es necesario que previamente se encuentren autorizados a través del Smart account del vendor. Solo así se permitirá que los equipos inicien el proceso de autenticación contra el equipo Vbond. Una vez autorizados se continua con el siguiente procedimiento

Paso 1. Configurar controladores.

En primer lugar, se debe poner en operación los controladores que manejaran la señalización y las instrucciones de enrutamiento. Para esto, desde el servidor de administración se debe asignar adjuntar el template con la configuración de los equipos controladores de la siguiente forma.

- Desde el módulo de administración se ingresa en la opción devices/controllers/add controller

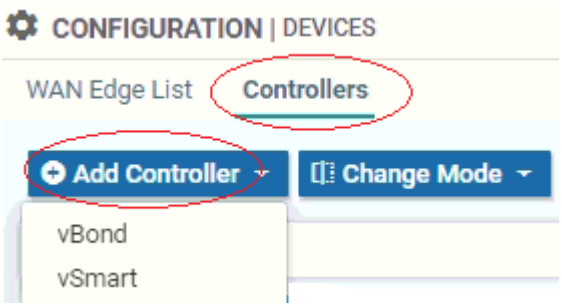


Figura 30. Agregar controlador en plataforma. (Autor,2021)

Después de esto la plataforma le solicitara confirmar la ip de gestión, un usuario y contraseña y el protocolo deseado para proteger la conexión bien sea TLS o DTLS. Una vez ingresada esa información se genera automáticamente la solicitud de firma de certificado (CSR) para que sea firmado por la entidad certificadora bien sea local o las entidades certificadoras internacionales.

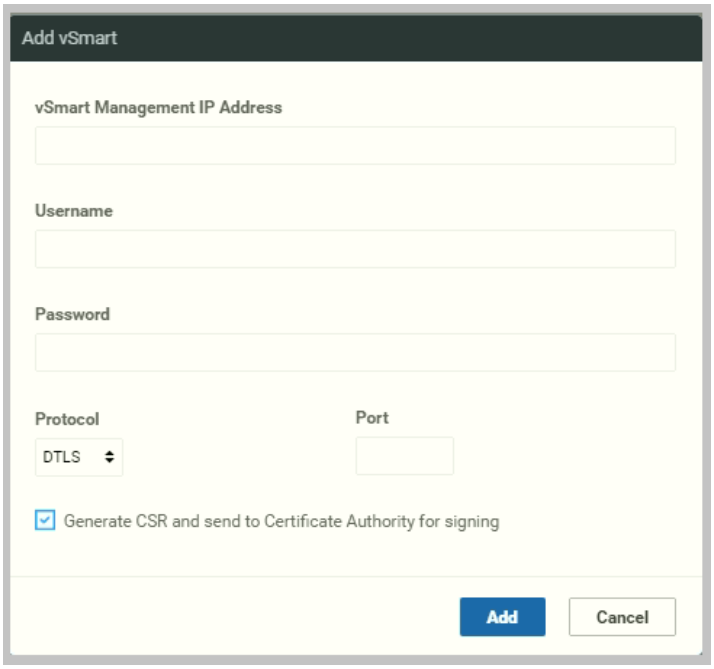


Figura 31. Opciones del controlador. (Autor,2021)

En este punto el controlador ya se encuentra preparado para recibir la configuración a través de la asignación de un témplate o a través de comandos.

Paso 2. Asignar configuración a los controladores

Para asignar la configuración correspondiente a los controladores se deben realizar los siguientes pasos en la plataforma de administración.

Ir a la opción configuración/templates y seleccionamos el template que se halla configurado para el controlador.

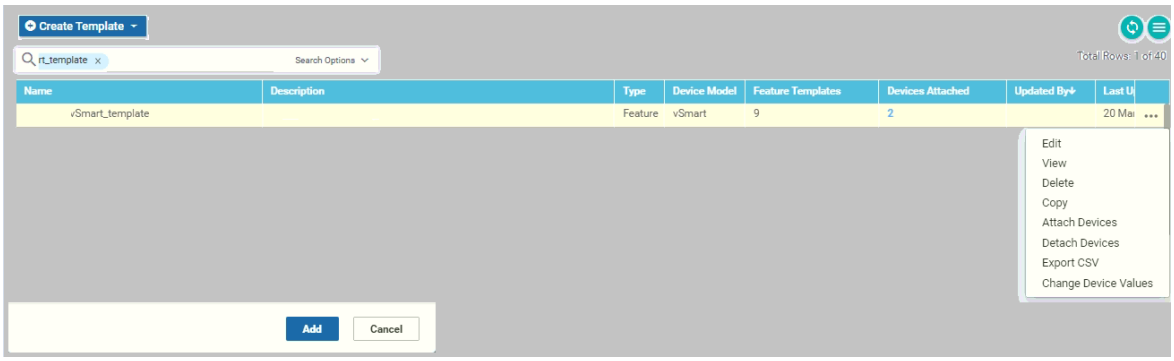


Figura 32. Asignación de template a controlador. (Autor,2021)

Seleccionamos los tres puntos en la parte derecha del template y seleccionamos la opción attach devices desplegando la ventana para ubicar el equipo al que queremos adjuntar el template. Con este paso los controladores cargan la configuración necesaria para realizar las funciones de control.

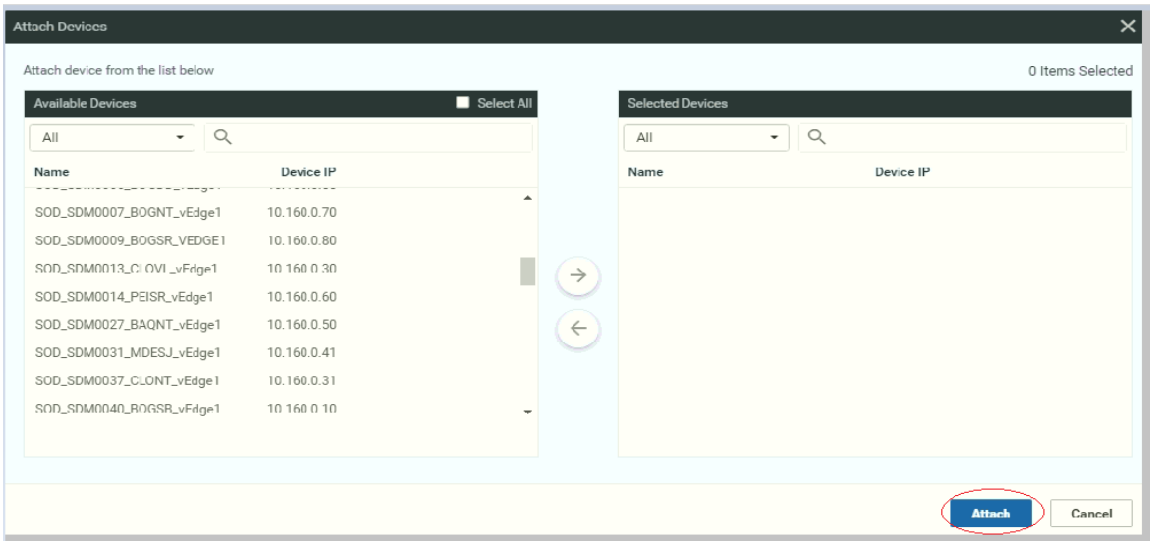


Figura 33. Proceso de asociación de template. (Autor,2021)

Paso 3. Subir equipos vedge 1000 de las sedes.

El proceso para subir los equipos del plano de datos a la red SD WAN es similar al proceso realizado con los controladores. En primer lugar, los equipos del plano de datos deben estar debidamente asociados al cliente (proceso que realiza el vendor). Una vez cumplido este paso se procede a subir el equipo mediante el siguiente procedimiento.

Se deben realizar las configuraciones básicas del sistema y la configuración de la vpn de transporte en el equipo para que pueda reconocer la infraestructura y hacer el proceso de autenticación. Dentro de esta configuración es importante el system ip, el site id y la unidad organizativa la cual debe ser la misma en todos los equipos. Esta configuración se realiza una sola vez por la línea de comandos ya que de ahí en adelante el equipo estará bajo el dominio de la plataforma de administración.

- **Configuración básica del sistema**

```
system
 description            SEDE_BARRANQUILLA
 host-name               SEDE_BARRANQUILLA
 system-ip               10.160.0.50
 site-id                 50
 admin-tech-on-failure
 no route-consistency-check
 sp-organization-name    Sodimac
 organization-name       Sodimac
 no port-hop
 clock timezone America/Bogota
 vbond vbond-1024177.viptela.net
```

- **Configuración de la VPN de transporte**

```
vpn 0
 name "Conexión de transporte"
 dns 200.14.207.210 primary
 dns 200.26.137.100 secondary
 host vbond-1024177.viptela.net ip x.x.x.x  → ip del vbond
 interface ge0/0
  no shutdown
  shaping-rate 140000
  qos-map      QoS_Map_Policy
 !
 interface ge0/0.531
```

```
 description "SDWAN Transport MPLS1" → Transporte a través de la MPLS
 ip address 10.168.31.42/30
 tunnel-interface
  encapsulation ipsec
  color private1 restrict
  mtu          1496
 no shutdown
!
interface ge0/1
 clear-dont-fragment
 no shutdown
 shaping-rate        70000
 qos-map             QoS_Map_Policy
!
interface ge0/1.444
 description "SDWAN INET TRANSPORT"    -→ Transporte a través del internet
 ip address 190.85.252.171/29
 tunnel-interface
  encapsulation ipsec
  color biz-internet restrict
  !
 mtu          1496
 no shutdown
!
interface ge0/4
 no shutdown
ip route 0.0.0.0/0 10.162.211.49
ip route 0.0.0.0/0 190.85.252.169
```

Paso 4. Adjuntar el témplate correspondiente a los equipos del plano de datos.

Con la configuración del paso 3 se logra que el vedge1000 del plano de datos haga la autenticación contra el Vbond y ya se encuentre disponible para recibir la configuración a través de la asignación del template. La asignación del template la realizamos de la siguiente forma:

En la opción configuración/templates ubicamos el ubicamos el template creado con la configuración y hacemos el proceso de asignación mediante la opción de la parte derecha tal como se realizado la asignación del témplate para los vSmart.

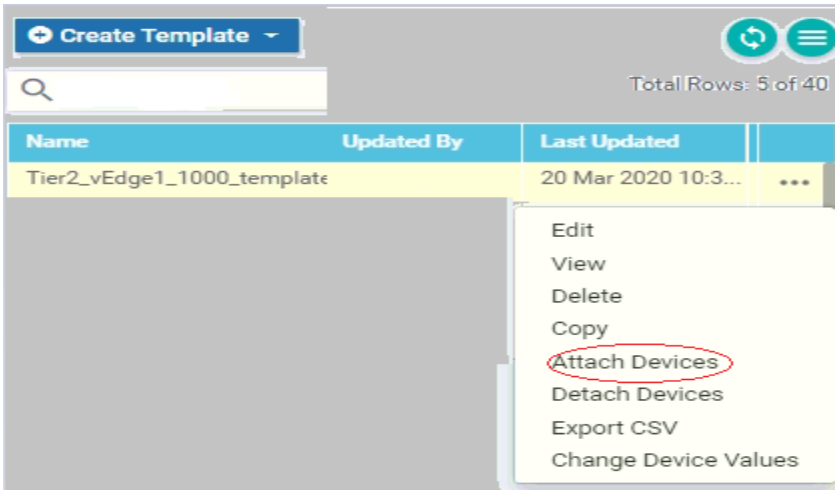


Figura 34. Asignación de template a Vedge. (Autor,2021)

7.3.1 Creación de los template

A diferencia de las redes tradicionales en donde la configuración se realiza a través de la línea de comandos, en SD WAN la configuración se puede realizar a través de plantillas o templates que contienen todas las características de configuración. De acuerdo al escenario propuesto la configuración para una de las sedes puede ser vista siguiente la siguiente ruta:

Configuración/devices buscamos el servicio y seleccionamos la opción change device values.

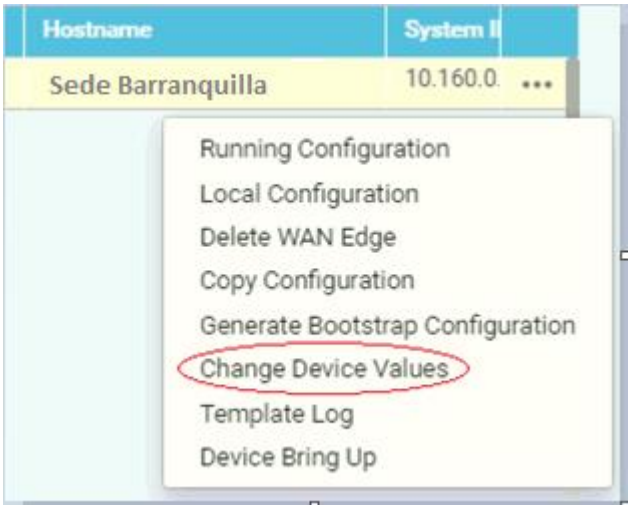


Figura 35. Modificando configuración de template. (Autor,2021)

Una vez dentro de esta opción podemos ver o modificar la configuración de acuerdo con el diseño de red que se halla diseñado.

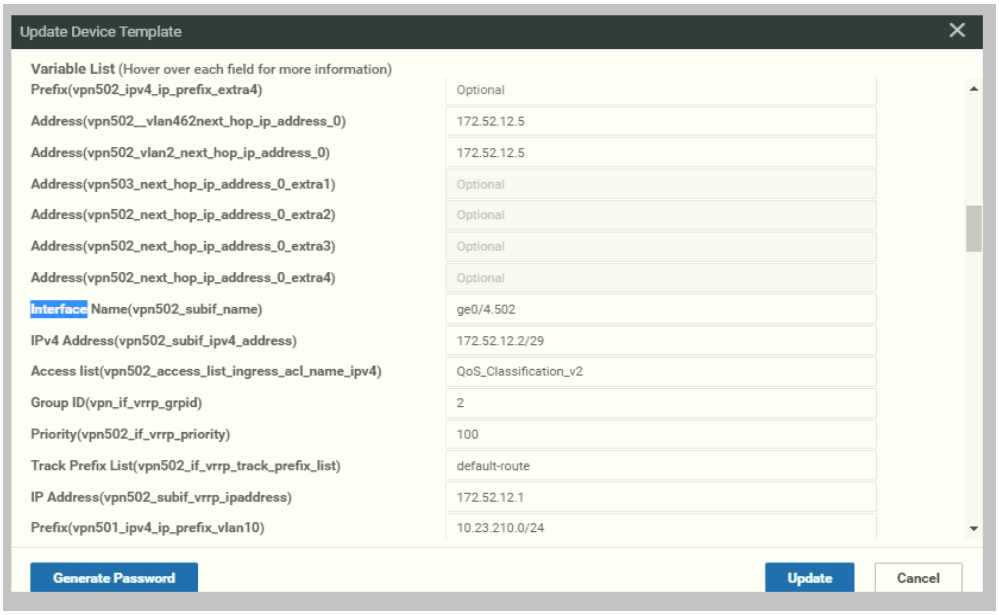


Figura 36. Template para una sede. (Autor,2021)

Así mismo se realiza se puede observar la configuración del template usado para el servicio de data center.

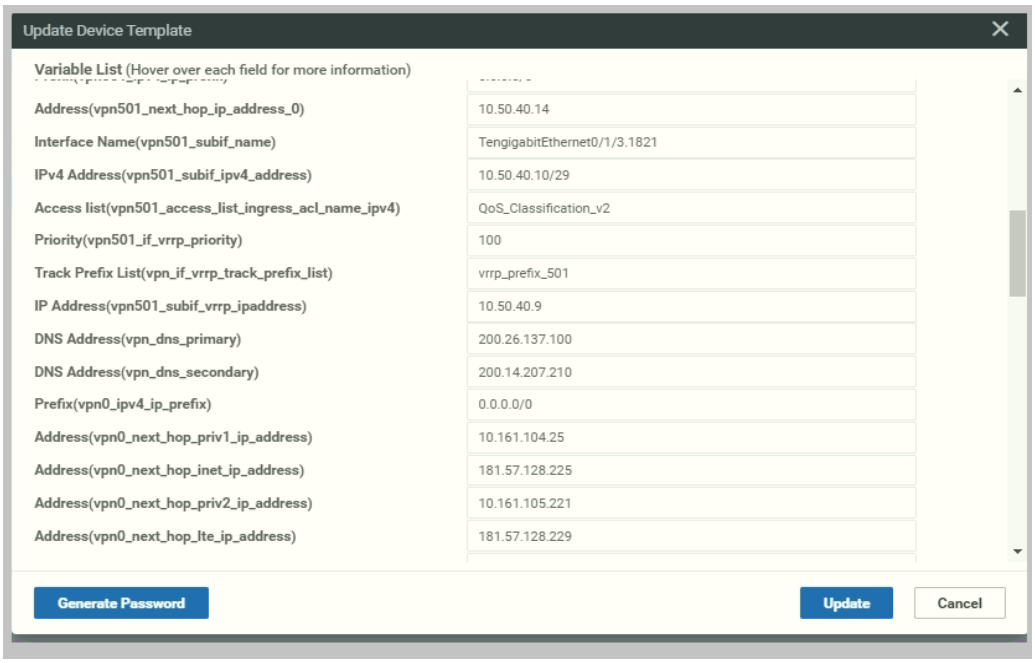


Figura 37. Template para data center. (Autor,2021)

7.4 Pruebas de operatividad

Finalizada la configuración se procede con las pruebas de servicio. En primer lugar, se verifica que las sesiones de control estén correctamente establecidas. Para esto vamos a ingresar al equipo Vedge del plano de datos y nos vamos a la opción control connections.

Ruta: Monitor/network buscamos el equipo y le damos click en control connections.

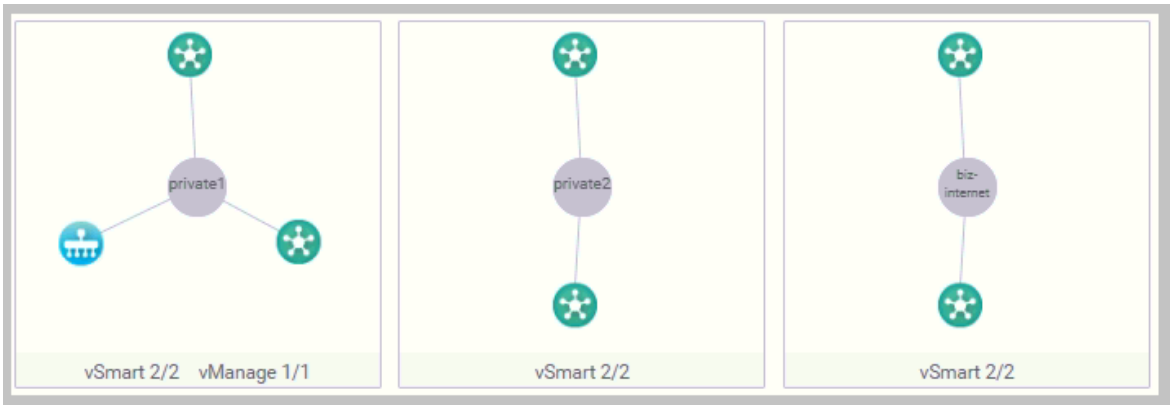


Figura 38. Sesiones de control. (Autor,2021)

Dentro del mismo equipo podemos verificar los túneles establecidos haciendo uso de la opción túnnel.

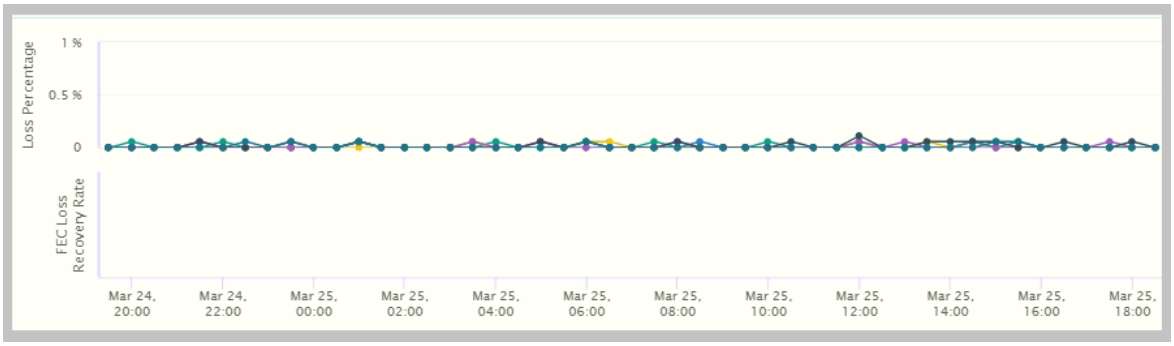
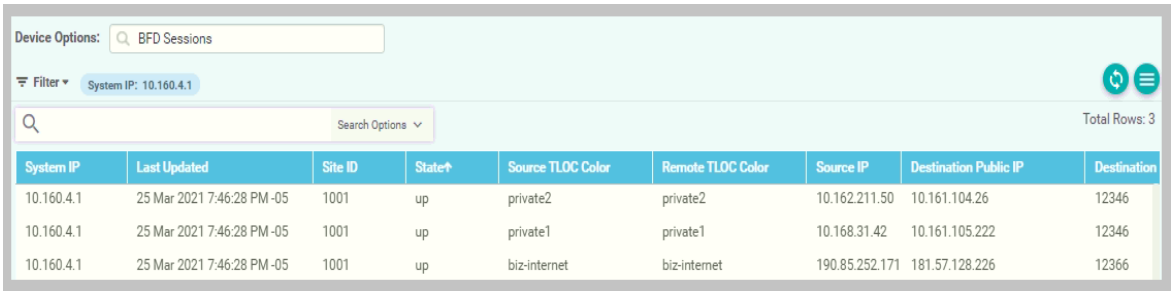


Figura 39. Trafico dentro del tunel. (Autor,2021)

Por último, se pueden realizar todas las funciones de verificación y diagnostico ingresando a la opción real time y seleccionando el mando de interés.



System IP	Last Updated	Site ID	State	Source TLOC Color	Remote TLOC Color	Source IP	Destination Public IP	Destination
10.160.4.1	25 Mar 2021 7:46:28 PM -05	1001	up	private2	private2	10.162.211.50	10.161.104.26	12346
10.160.4.1	25 Mar 2021 7:46:28 PM -05	1001	up	private1	private1	10.168.31.42	10.161.105.222	12346
10.160.4.1	25 Mar 2021 7:46:28 PM -05	1001	up	biz-internet	biz-internet	190.85.252.171	181.57.128.226	12366

Figura 40. Establecimiento de sesiones BFD. (Autor,2021)

Conclusiones

Mediante el análisis de la relación entre los componentes de las redes basadas en software se evidencia una evolución hacia una red más flexible y escalable que hace uso de protocolos estandarizados que contribuyen al establecimiento de la señalización entre los diferentes componentes de la red. Estos protocolos se encargan de transportar la información necesaria para asegurar que la comunicación de extremo a extremo se realice de forma adecuada y con los niveles de calidad configuradas en las políticas de QoS. Así mismo todos los componentes involucrados dentro de la solución mantienen un vínculo directo con el servidor de administración con el propósito de mantener actualizadas las estadísticas de los enlaces activos.

Las redes basadas en software simplifican el diseño de mecanismos de seguridad a nivel WAN mediante la inclusión de diferentes características implícitas dentro de su implementación. El alcance a nivel de seguridad cubre todo el tráfico enviado a través de este tipo de redes, tanto de usuario como de control. El tráfico de usuario entre los diferentes nodos de la red se transporta de forma segura haciendo uso de IP SEC mientras que el tráfico de control se encuentra protegido por el uso de conexiones DTLS y DTLS en la capa de transporte.

La separación de planos es una de las características más llamativas de las redes basadas en software ya que mediante este diseño se proporciona una mayor escalabilidad haciendo uso de un plano de control independiente que es capaz de soportar un gran número de equipos encargados del reenvío de tráfico. Esta característica disminuye los costos operativos y facilita la implementación de

nuevos servicios mediante mecanismos de aprovisionamiento automático como Zero touch provisioning (ZTP).

La administración de la red se simplifica de manera notable gracias al plano de administración que se encarga de monitorear los equipos y las conexiones establecidas. El módulo de administración facilita la gestión de la red mediante el uso de una interface web en donde no solo se pueden analizar estadísticas, sino que también permite la implementación de nuevos servicios haciendo uso de protocolos de administración de red como NETCONF. Los módulos de monitoreo, configuración, herramientas, mantenimiento, administración y análisis contienen diversas funciones que engloban la administración total de la red en términos de Calidad, flexibilidad y seguridad.

Bibliografía

Álvarez, C. (2016). *El concepto de Hashing Algorithm*. https://www.arquitecturajava.com/el-concepto-de-hashing-algorithm/

Arizmendi, L. (2014). *Ideas para datacenters*. http://luisarizmendi.blogspot.com/2014/08/vxlan-redes-virtuales-overlay.html

Baluja, W. (2011). *Arquitectura de Seguridad para las redes de Telecomunicaciones*. https://www.researchgate.net/publication/279639318_Arquitectura_de_Seguridad_para_las_redes_de_Telecomunicaciones

Barozet, J. (2017). *Cisco SD WAN Deep Dive*.

Bialy, M. (2020). *How does Zero-Touch-Provisioning (ZTP) in Cisco SD-WAN work?* https://www.grandmetric.com/2020/03/23/zero-touch-provisioning-ztp-cisco-sd-wan-work/

Bustos, C. (2019). *Análisis de Factibilidad Técnico y Económico entre una red MPLS Trafic Engineering (TE) con ipsec y una red sd wan*. *C*, 1. https://repositorio.espe.edu.ec/bitstream/21000/13743/5/T-ESPE-057806.pdf%0Ahttp://repositorio.espe.edu.ec/bitstream/21000/10846/1/T-ESPE-049674.pdf

Ceballos, A., Bautista, F., Mesa, L., & Argaez, C. (2019). *Tendencias cibercrimen Colombia 2019 - 2020*. https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

CEPAL. (2014). *Cloud computing in Latin America: Current situation and policy proposalstle*.

Cisco. (2008). *Data Plane Security Overview*. https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/Security/01Security_Overview/Data_Plane_Security_Overview

Cisco. (2019). *The Role of Dynamic IPsec Tunnels in Modern SD-WAN Networks White Papere*. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white-paper-c11-743108.html

Cisco. (2020a). *Cisco SD-WAN Design Guide*. https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html

Cisco. (2020b). *SD-WAN Command Reference*.

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/operational-cmd.html

Craven, C. (2019). *SD-WAN as a Service Using Orchestration – Definition*. https://www.sdxcentral.com/networking/sd-wan/definitions/sd-wan-orchestration/

Dclessons. (2020). *SD-WAN Viptela Templates*. https://www.dclessons.com/sd-wan-viptela-templates

Delivery, R. W. A. N., & Era, C. (2019). *Cisco Software-Defined WAN for Secure Networks*.

Feamster, N. (2014). *The Road to SDN*. https://queue.acm.org/detail.cfm?id=2560327

Feamster, N., Rexford, J., & Zegura, E. (2014). *The Road to SDN An Intellectual History of programable Networks*. https://doi.org/10.1145/2602204.2602219

Gil, M. (n.d.). *Los orígenes de SD-WAN: el proyecto Clean Slate*. Retrieved May 10, 2020, from https://www.teldat.com/blog/es/internet-solucion-sd-wan-sdn-red-ip-plano-de-control-y-datos/

IBM. (2018). *Implementación de SD-WAN en el Mundo Real*.

Infante, C. (n.d.). *Escalabilidad de red para la era digital*. Retrieved May 10, 2020, from https://gblogs.cisco.com/es/2019/01/escalabilidad-de-red-para-la-era-digital/

Kent, S. (2005). *IP Encapsulating Security Payload (ESP)*. https://www.hjp.at/doc/rfc/rfc4303.html#sec_1

Khabarov, E. (2019). *Configure Connectivity Between Different TLOC Colors*. https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214148-configure-connectivity-between-different.html

Lanner. (n.d.). *3 Opciones de Implementación de SD-WAN para Empresas que Deseen Invertir en SDN | Lanner*. Retrieved May 10, 2020, from https://www.lanner-america.com/es/blog-es/3-opciones-de-implementacion-de-sd-wan-para-empresas-que-deseen-invertir-en-sdn/

Marshall, C. (2019). *Overlay Management Protocol (OMP)*. https://www.lookingpoint.com/blog/cisco-sd-wan-omp

MinTIC. (2018). Plan TIC 2018-2022. *El Futuro Digital Es de Todos*, 1–105.

https://www.mintic.gov.co/portal/604/articles-101922_Plan_TIC.pdf

MinTIC. (2020). *Regulación de Comunicaciones*. https://www.mintic.gov.co/portal/inicio/4033:Comisi-n-de-Regulaci-n-de-Comunicaciones

O.N.F. (2012). Software-defined networking: The new norm for networks. *ONF White Paper*, *2*, 2–6.

Reseller, I. (2018). *Como resolver los problemas a los que se enfrentan las redes tradicionales*. https://www.itreseller.es/content-marketing/2018/02/como-resolver-los-problemas-a-los-que-se-enfrentan-las-redes-tradicionales

Rodríguez, J. (2008). *SD-WAN, la respuesta a las necesidades de la red empresarial*. https://www.citrix.com/content/dam/citrix/en_us/documents/solution-brief/sd-wan-the-answer-to-networking-demands-es.pdf

Rouse, M. (2013). *Netconf*. https://searchnetworking.techtarget.com/definition/NETCONF

Sanchis, J. (2018). *Viptela: simplifica la gestión de tu red WAN*. https://www.sothis.tech/viptela-dar-solucion-al-aumento-dispositivos-conectados-la-red/

SIC. (n.d.). *Proteccion al consumidor*. https://www.sic.gov.co/objetivos-y-funciones

Staff. (2016). *La adopción de redes basadas en software ya está ocurriendo*. https://www.tynmagazine.com/la-adopcion-de-redes-basadas-en-software-ya-esta-ocurriendo/

Ueno, D. (2020). *Understanding the DTLS all-zero ClientHello.random vulnerability*. https://www.redhat.com/en/blog/understanding-dtls-all-zero-clienthellorandom-vulnerability

Vector. (2018). El crecimiento del Cloud Computing es más rápido de lo esperado. *Vector Itc*. https://www.vectoritcgroup.com/tech-magazine/software-trends/el-crecimiento-del-cloud-computing-es-mas-rapido-de-lo-esperado/